Date de réception : 23/01/2015

Published ID	:	C-362/14
Document number	:	13
Register number	:	976996
Date of lodgment	:	03/11/2014
Date of entry in the register	:	03/11/2014
Type of document	:	Observations
	:	Document
Lodgment reference	:	DC33346
File number	:	1
Person lodging document	:	Julie Vondung (R249125) Commission

EUROPEAN COMMISSION

LEGAL SERVICE

Brussels, 3 November 2014
sj.f(2014)4003332

Court procedural documents

TO THE PRESIDENT AND THE MEMBERS OF THE COURT OF JUSTICE OF THE EUROPEAN UNION

WRITTEN OBSERVATIONS

submitted by

THE EUROPEAN COMMISSION

represented by Mr Ben Smulders, Principal Legal Adviser, Mr Bernd Martenczuk and Ms Julie Vondung, members of its Legal Service, acting as agents, with an address for service at the office of Ms Merete Clausen, also a member of its Legal Service, Bâtiment Bech, 5 rue A. Weicker, L-2721 Luxemburg, and which consents to service by e-Curia,

in Case C-362/14,

Request for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings

Maximilian Schrems

v

Data Protection Officer,

amicus curiae:

Digital Rights Ireland Ltd.

on the interpretation of Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

TABLE OF CONTENTS

The European Commission has the honour to present the following written observations:

1. INTRODUCTION AND SUMMARY

1. The questions referred concern the powers and duties of national data protection authorities under the Safe Harbour Decision[1] following the Snowden revelations on large-scale surveillance programmes of US national security agencies. In the Safe Harbour Decision, the European Commission found in 2000 that US companies subscribing to the privacy principles set out therein ensure an adequate level of protection of personal data and, consequently, personal data can be transferred to these companies according to Directive 95/46/EC on the protection of personal data. The surveillance programmes, the existence of which were revealed in 2013 by whistle-blower Edward Snowden, allow US national security agencies to access personal data transferred to US companies – among which Facebook Inc. - on a mass and indiscriminate basis. Following these revelations the Commission has started to review the Safe Harbour Decision, a process which is still ongoing.

2. The Applicant in the main proceedings, Maximilian Schrems, challenges the refusal of the respondent Irish data protection authority, the Data Protection Commissioner, to investigate further his complaint on the transfer of his personal data by Facebook Ireland Ltd to Facebook Inc. in the US, which has self-certified under Safe Harbour. He is arguing that due to the surveillance programmes (under which PRISM) an adequate level of protection is not ensured anymore and thus such transfer is unlawful. The Respondent contends that he is bound by the finding of the Commission to the contrary in the Safe Harbour Decision. The High Court, in essence, asks whether, in the light of the Charter of Fundamental Rights, the Data Protection Commissioner is indeed absolutely bound by this finding or, alternatively, whether he may and/or must conduct his own investigations in the light of the Snowden revelations.

---

[1] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ L 215, 25.08.2000, p. 7 – 47).

3. The Commission considers that the Snowden revelations indeed raise serious concerns with a view to the application of the Safe Harbour Decision. For this reason, it has taken action and started the review of the Safe Harbour Decision, as will be presented more in detail later. However, in the Commission's view, a national data protection authority is bound by the Commission's adequacy finding as long as the Safe Harbour Decision itself does not allow the contrary according to its Article 3 (1). Under Article 3 (1) (b), national data protection authorities may in particular suspend data flows to a self-certified organisation "*where there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.*" Under circumstances such as in the case before the national court, these conditions are only partially met. Whereas, in the light of the Snowden revelations, "*a substantial likelihood that the Safe Harbour Principles are being violated*" and "*a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue*" do exist, there are no indications that the continuing transfer of personal data of the Applicant by Facebook Ireland Limited to Facebook Inc would create "*an imminent risk of grave harm*" to the Applicant.

2. LEGAL FRAMEWORK

4. The legal framework set out by the law of the European Union relevant to the present case is composed of Articles 7, 8 and 47 of the Charter of Fundamental Rights, Art. 25 of Directive 95/46/EC and the Safe Harbour Decision.

2.1. The Charter of Fundamental Rights

5. Article 7 of the Charter is drafted as follows:

> Respect for private and family life
>
> Everyone has the right to respect for his or her private and family life, home and communications.

6. Article 8 of the Charter is drafted as follows:

> Protection of personal data
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

7. Article 47 of the Charter is drafted as follows:

> Right to an effective remedy and to a fair trial
>
> Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.
>
> Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.
>
> Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

2.2. Directive 95/46/EC

8. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31 – 50) governs the transfer of personal data to third countries. According to Article 25 of Directive 95/46/EC, in principle, such transfer is only admissible if the third country ensures an adequate level of protection. The Commission may find under Article 25 (6) that a third country ensures such an adequate level of protection; transfers of personal data to this third country are consequently admissible without the necessity of providing additional guarantees. Member States are obliged to comply with the Commission's decision as regards the recognition of the level of protection offered in that country (Article 25 (6), last sub-paragraph).

9. Article 25 of Directive 95/46/EC is drafted as follows:

> Principles
>
> 1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other

provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

2.3. Decision 2000/520/EC (Safe Harbour Decision)

10. The Safe Harbour Decision is based on Article 25 (6) of Directive 95/46/EC.

11. According to Article 1, the Safe Harbour Decision governs the transfer of personal data from the EU to organisations established in the US that have self-certified to the Safe Harbour Privacy Principles as set out in Annex I to the Decision and implemented in accordance with the guidance provided by the Frequently Asked Questions (FAQs) issued by the US Department of Commerce as set out in Annex II of the Decision. The Commission's Decision recognises according to Article 1(1) the Privacy Principles and the accompanying FAQs as ensuring an adequate level of protection for personal data transfer to US companies in the US.

12. The fourth paragraph in the preamble to the Privacy Principles issued by the US Department of Commerce and contained in Annex I of the Safe Harbour Decision states:

Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; ...

13. Annex III of the Decision sets out an overview of the Safe Harbour enforcement. According to Annex VII, the US Federal Trade Commission and the Department of Transportation are empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case on non-compliance with the Principles implemented in accordance with the FAQs.

14. Furthermore, the Safe Harbour Decision outlines and distinguishes respective powers of, on the one hand, the European Commission, and on the other, national data protection authorities of the Member States.

15. The powers of the Commission are referred to in recital 9 and set out in Article 4 of the Safe Harbour Decision.

16. Recital 9 reads as follows:

> The "safe harbor" created by the Principles and the FAQs, may need to be reviewed in the light of experience, of developments concerning the protection of privacy in circumstances in which technology is constantly making easier the transfer and processing of personal data and in the light of reports on implementation by enforcement authorities involved.

17. Article 4 states in relevant part:

> 1. This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation.
>
> The Commission shall in any case evaluate the implementation of the present Decision on the basis of available information three years after its notification to the Member States and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the evaluation that the provisions set out in Article 1 of this Decision provide adequate protection within the meaning of Article 25 of Directive 95/46/EC and any evidence that the present Decision is being implemented in a discriminatory way.
>
> 2. The Commission shall, if necessary, present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46/EC.

18. The powers of data protection authorities in the Member States are referred to in recital 8 and set out in Article 3 (1) of the Safe Harbour Decision.

19. Recital 8 reads as follows:

> In the interests of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify in this Decision the exceptional circumstances in which the suspension of specific data flows should be justified, notwithstanding the finding of adequate protection.

20. Article 3 (1) states in relevant part:

> 1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data in cases where:
>
> (a) ...; or
>
> (b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.
>
> The suspension shall cease as soon as compliance with the Principles implemented in accordance with the FAQs is assured and the competent authorities concerned in the Community are notified thereof.

21. Additionally, Article 3 (2) specifically requires that Member States shall inform the Commission without delay when measures are adopted on the basis of paragraph 1.

3. THE COMPLAINT IN THE MAIN PROCEEDINGS AND THE QUESTIONS REFERRED FOR A PRELIMINARY RULING

22. The Applicant, an Austrian national, challenges a decision of the Respondent, the Irish Data Protection Commissioner, not to investigate further the merits of his complaint brought in the wake of the revelations in June 2013 of the mass surveillance of internet and telecommunications data by the US national security agencies ("the Snowden revelations"). The Applicant has been a customer of the social networking service "Facebook" operated by Facebook Ireland Ltd since 2008. Facebook Ireland Ltd transfers some or all data of its customers to its parent company in the United States of America, Facebook Inc. Facebook Inc. is self-certified under the Safe Harbour Regime. The essence of Mr Schrems' complaint to the Respondent was that, in light of the Snowden revelations,

there was no meaningful protection in US law and practice in respect of data transferred by the company Facebook Ireland to its US parent company so far as State surveillance was concerned. He did not raise any special implications of the mass surveillance for his own situation.

23. In assessing the complaint, the Commissioner did not find evidence that Mr Schrems' own personal data had been disclosed to the US (*locus standi* objection). The Commissioner further took the view that the question of observance of data protection standards by the US was foreclosed by the Safe Harbour Decision of the European Commission.

24. The High Court, having rejected the *locus standi* objection, found that the Commissioner has *"demonstrated scrupulous steadfastness to the letter of the 1995 Directive and the 2000 Decision*" and stressed that neither the validity of Directive 95/46/EC nor the Safe Harbour Decision have been challenged. According to the referring court, Article 3 (1) (b) of the Safe Harbour Decision was not applicable to the case as the complaint was not directed to the *conduct* of Facebook itself.[2] The referring court's questions and doubts about the approach taken by the Commissioner stem from developments that have taken place in the 14 years since the adoption of the Safe Harbour Decision, namely technological advancements, the Snowden revelations and, since 2009, the binding nature of the Charter of Fundamental Rights of the European Union, in particular Articles 7, 8 and 47.

25. Furthermore, the referring court stated that "if the matter were to be judged solely by reference to Irish constitutional law standards, the Commissioner could not properly have exercised his s. 1O(1)(a) powers to conclude in a summary fashion that there was nothing further to investigate".[3] As noted by the referring court, under Irish national law, "the accessing of private communications by the State authorities through interception or surveillance engages the constitutional right to privacy. Further, accessing by State authorities of private communications generated within the home [...] is also a clear interference with the inviolability of the dwelling as guaranteed by Article 40.5 of the

---

2 See paragraph 19 of the request for a preliminary ruling.

3 See paragraph 15 of the request for a preliminary ruling.

Constitution".[4] However, as the matter concerned was covered by EU legislation and Irish law thus precluded, the referring court decided to submit a request for a preliminary ruling to the CJEU.

26. The High Court consequently stayed its proceedings and referred the following questions for a preliminary ruling:

> "Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC) having regard to Article 7, Article 8 and Article 47 of the Charter of Fundamental Rights of the European Union (2000/C 364/01), the provisions of Article 25(6) of Directive 95/46/EC notwithstanding? Or, alternatively, may and/or must the once holder conduct his or her own investigation of the matter in the light of actual developments in the meantime since that Commission Decision was first published?"

4. THE REACTION OF THE EUROPEAN COMMISSION TO THE SNOWDEN ALLEGATIONS

27. Since June 2013, the existence of a number of US surveillance programmes involving the large-scale collection and processing of personal data has been revealed. The programmes concern in particular the collection of personal data from US internet and telecommunication service providers and the monitoring of data flows inside and outside the US. Given the central position of these US companies in the EU market, the transatlantic routing of a large part of electronic data flows and communications, and the volume of electronic data flows across the Atlantic, a very significant number of

---

[4] Paragraph 9 of the request for a preliminary ruling.

individuals in the EU, and most likely all users of the internet in Europe, may be affected by these programmes.

28. Following these revelations, the Commission immediately expressed serious concerns and requested clarifications from the US both orally and in writing regarding the impact of these programmes on the fundamental rights of individuals in the EU, specifically their right to privacy and to the protection of personal data. In particular, an ad hoc EU-US working group on data protection[5] was set up in July 2013 to establish the facts surrounding the revelations. A report of the Working Group was published on 27 November 2013 (ANNEX 1). [6] The US confirmed that it is under Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA) that the National Security Agency (NSA) maintains a database known as PRISM which allows collection of electronically stored data. [7] The US also confirmed that Section 702 provides the legal basis for the so-called "upstream collection"; this is understood to be the interception of Internet communications by the NSA as they transit to or through the US (e.g. through cables, at transmission points). The US further confirmed that Executive Order 12333 is another legal basis for other surveillance programmes for the broad mass collection of data from the internet and is the general framework on intelligence gathering inside and outside the US.[8]

29. On the same day, the Commission issued two communications which respectively assessed the functioning of the Safe Harbour (ANNEX 2)[9] and set out a series of action to

---

5 The group was co-chaired by the Commission and the Presidency of the Council and with, inter alia, the participation of the EEAS, Member States' experts and representatives of the relevant US government authorities.

6 Report of the Findings by the EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf

7 See section 2.1.1 of the Report of the EU-US ad hoc High Level Working Group. PRISM allows collection of electronically stored data, including content data, by means of directives addressed to the main US internet service providers and technology companies providing online services, including, according to classified documents disclosed in the press but not confirmed by the US, Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Apple, Skype and YouTube.

8 See section 2.3 of the Report of the EU-US ad hoc High Level Working Group.

9 Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU", COM(2013) 847, 27.11.2013.

be taken in order to restore trust in data flows between the EU and the US (ANNEX 3)[10]. The Communication on the Functioning of Safe Harbour identified 13 recommendations, addressed to the US, aimed at strengthening the Safe Harbour framework in light of developments that have taken place since its adoption. Recommendations 1-11 address basic obligations of the Safe Harbour framework and fall into three categories: transparency, redress and enforcement. Recommendations 12 and 13 relate to the need to address the question of access by US authorities to Safe Harbour data for national security purposes, in particular in the context of the national security exemption contained in the current Safe Harbour framework. Number 12 states: "*Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.*" Number 13 states: "*It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate*".[11]

30. In its Communication on rebuilding trust in EU-US data flows, the Commission outlined three policy options vis-à-vis the Safe Harbour: maintaining the status quo, strengthening the Safe Harbour scheme and reviewing its functioning thoroughly and suspending or revoking the Safe Harbour decision. The Commission is currently actively engaged with the US government authorities to discuss the implementation by the US of the 13 recommendations set out in the Communication. Given the sensitivity and complexity of the issues at hand, discussions are ongoing.

---

[10] Communication from the Commission to the European Parliament and the Council, "Rebuilding Trust in EU-US Data Flows", COM(2013) 846, 27.11.2013. The main measures of the package are: (1) a swift adoption of the EU's data protection reform; (2) making Safe Harbour safe; (3) strengthening data protection safeguards in the law enforcement area (umbrella agreement); (4) using existing Mutual Legal Assistance and sectoral agreements to obtain data; (5) addressing European concerns in the on-going U.S. reform process on intelligence gathering activities; and (6) promoting privacy standards internationally.

[11] COM(2013) 847, p. 18.

5. LEGAL ANALYSIS

5.1. General Observations

31. In accordance with Article 25 (6), last subparagraph, of Directive 95/46/EC, adequacy decisions are in principle binding on all Member States. Article 3 (1) (b) of the Safe Harbour Decision allows national data protection authorities under certain conditions to suspend data flows to the US. This provision is an exception to the uniform application of the Commission's adequacy decision and therefore, in principle, must be interpreted restrictively. At the same time, it has to be interpreted in the light of the Charter, especially of Articles 7 and 8 thereof.

32. Moreover, in the interpretation of Article 3 (1) (b), it is important to take into account the relationship of the respective powers of the Commission and of the national data protection authorities. In particular, as will be explained in more detail below, the competences of the national data protection authorities are focused on the application of data protection law in individual cases whereas the general review of the application of the Safe Harbour Decision including any decisions as regards its suspension or termination fall under the competences of the Commission.

5.2. The conditions of Article 3 (1) (b) of the Safe Harbour Decision are only partly met

33. Pursuant to Article 3 (1) (b) of the Safe Harbour Decision, there are four cumulative conditions under which the DPAs can decide to suspend specific data flows:

5.2.1. First condition: There is a substantial likelihood that the Principles are being violated

34. In the Commission's view, a substantial likelihood that the Safe Harbour Principles have been violated does exist. The very large-scale and indiscriminate nature of the US mass-surveillance programmes is namely incompatible with the strictly tailored national security exemption in the Safe Harbour Principles as set out in the fourth paragraph of the preamble to the Privacy Principles.

35. This conclusion follows from an interpretation of the Safe Harbour Decision in the light of the Charter of Fundamental Rights and the relevant case law of the Court. According to Article 52(1) of the Charter, *"any limitation on the exercise of the rights and freedoms*

recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." Equally, under the European Convention on Human Rights "*there shall be no interference by a public authority with the exercise of* the right" to respect for private and family life, which includes the right to data protection, "*except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"* (Article 8 (2) thereof). According to the case law of the Court on the right to respect for private life:

"*(...) the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary*".[12]

36. Consequently, the Safe Harbour Decision which specifies that such limitations are allowed only "*to the extent necessary*" to meet national security, public interest, or law enforcement requirements, must be interpreted *strictly*.

37. As the Court has repeatedly held, the exception foreseen in Article 4 (2) TEU, according to which national security remains the sole responsibility of each Member States, cannot lead to setting aside EU law (cf. Case C-300/11, *ZZ v. Secretary of State for the Home Department*, para. 38[13]). Furthermore, the Court also held that the limits of Article 52 (1) of the Charter of Fundamental Rights apply also in this area of law; see, for instance paragraphs 49 and 51 in Case C-300/11, *ZZ v. Secretary of State for the Home Department*:

"*It is only by way of derogation that Article 30(2) of Directive 2004/38 permits the Member States to limit the information sent to the person concerned in the interests of*

---

12 See Case C-293/12, *Digital Rights Ireland*, EU:C:2014:238, paragraph 52.

13 EU:C:2013:363.

State security. As a derogation from the rule set out in the preceding paragraph of the present judgment, this provision must be interpreted strictly, but without depriving it of its effectiveness. [...] In particular, it should be taken into account that, whilst Article 52(1) of the Charter admittedly allows limitations on the exercise of the rights enshrined by the Charter, it nevertheless lays down that any limitation must in particular respect the essence of the fundamental right in question and requires, in addition, that, subject to the principle of proportionality, the limitation must be necessary and genuinely meet objectives of general interest recognised by the European Union".

38. This reasoning holds all the more true, as the present case concerns the use of a national security exemption for the benefit of a *third country*, here the U.S., which is contained in a decision of the European Commission. The present case therefore does not concern the responsibilities of Member States in the maintenance of their national security.

39. Of relevance in this context is moreover the Court's judgment in Case C-293/12, *Digital Rights Ireland*, where it held in paragraph 37:

"*It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.* "

40. Furthermore, by way of analogy in the specific context of criminal law enforcement the CJEU held in the same judgment, para. 51, that the:

"*fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.*"

41. Against this background the Court considered that there was a manifest violation of the principle of proportionality and consequently an unlawful interference with the right to personal data protection insofar as:

a) the retention of personal data affected, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions (para. 58);

b) Directive 2006/24 did not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it was not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences (para. 59).

c) Not only there was a general absence of limits in Directive 2006/24 but also of any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference (para. 60).

42. The Snowden revelations on mass surveillance (the veracity and seriousness of which the referring Court has acknowledged), the publication in the press of a series of official documents, including classified documents, a number of which were subsequently declassified and made public by the US government, as well as the findings of the EU-US Ad Hoc High Level Working Group point to a scale of mass surveillance that, in the words of the referring court itself "*demonstrate a massive overreach on the part of the security authorities, with an almost studied indifference to the privacy interests of ordinary citizens [whose] data protection rights have been seriously compromised by*

mass and largely unsupervised surveillance programmes".[14] The surveillance programmes do not contain any limitations either with regard to the persons concerned or the type of personal data collected. The large-scale nature of the surveillance programmes may thus indeed result in data transferred under Safe Harbour being accessed and further processed by US authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in the Safe Harbour Decision.

43. Furthermore, Facebook is self-certified under Safe Harbour and implicated in the PRISM programme.[15] In this context, contrary to the views of the referring court,[16] it is irrelevant whether Facebook Inc. itself has (directly or knowingly) violated the Principles. From the point of view of the protection of EU data subjects' rights it is only relevant whether the level of protection that an adequacy finding is meant to guarantee has been undermined regardless of the fact of whether this is the result of an action by a company or by a public authority.

44. In light of these facts, it must be established that there is a substantial likelihood that adherence to the Safe Harbour Privacy Principles have been limited in a way that fails to comply with the strictly tailored national security exemption. The revelations in question point to a level of surveillance of a massive and indiscriminate scale incompatible with the standard of necessity laid down in that exemption as well as, more generally, with the right to personal data protection as enshrined in Article 8 of the Charter.

45. Accordingly, in light of the above and the nature and extent of the surveillance programmes at issue, there is a substantial likelihood that the Principles laid down in the Safe Harbour Decision have been violated under circumstances such as in the main proceedings.

---

[14] Judgment of the High Court of 18th June, 2014, *Schrems v. Data Protection Commissioner* [2014] IECCA 68, point 8.

[15] See section 2.1.1 of the Report of the EU-US ad hoc High Level Working Group. PRISM allows collection of electronically stored data, including content data, by means of directives addressed to the main US internet service providers and technology companies providing online services, including, according to classified documents disclosed in the press but not confirmed by the US, Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Apple, Skype and YouTube: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

5.2.2. *Second condition:* There is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue

46. According to the second condition of Article 3 (1) (b) of the Safe Harbour Decision, there must be a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue.

47. The enforcement of the Safe Harbour framework rests primarily with the US Federal Trade Commission. However, the enforcement mechanism of the Safe Harbour has no authority to intervene as regards surveillance programmes in general and in particular on the question whether the necessity condition of the exemption is complied with. The scope of the surveillance programmes and the conditions under which they operate are fixed by the US national security agencies under the control of the Director of National Intelligence and only some programmes are subject to the judicial oversight of the US Foreign Intelligence Surveillance Court (FISC). It is worth recalling that the FISC proceedings are non-adversarial and there is no representation before the Court of the interests of the data subject during the consideration of an application for an order.[17] It follows from the above that the enforcement mechanism is not able to take adequate and timely steps to settle the possible surveillance under the surveillance programmes by US national security agencies of the complainant's personal data in Facebook.

48. Accordingly, there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue under circumstances such as in the main proceedings.

5.2.3. *Third condition:* The continuing transfer would create an imminent risk of grave harm to data subjects

49. According to the third condition of Article 3 (1) (b) of the Safe Harbour Decision, the continuing transfer of personal data has to create an imminent risk of grave harm to data subjects.

---

[16] Cf. above para. 23.

[17] See the Report of the EU-US Ad hoc Working Group on Data Protection (section 4.3).

50. When interpreting this condition, the general observations on the interpretation of Article 3 (1) (b) as set out above have to be kept in mind. Being an exception to the uniform application of the Commission's adequacy decision, this provision, in principle, has to be interpreted restrictively. Moreover, as already noted, in the interpretation of Article 3 (1) (b), it is important to take into account the relationship of the respective powers of the Commission and of the national data protection authorities. In particular, the competences of the national data protection authorities are focused on the application of data protection law in individual cases whereas the general review of the application of the Safe Harbour Decision including any decisions as regards its suspension or termination fall under the competences of the Commission. This means in particular that the conditions set out in Article 3 (1) (b) have to be fulfilled in the specific circumstances at hand, as recital 8 of the Safe Harbour Decision (*"suspension of specific data flows"*).

51. In this regard, it must be underlined that "grave harm" indicates a higher level of damage or prejudice than the mere violation of the right to the protection of personal data. The language rather points to a qualified prejudice. Also, a systematic reading with the first condition shows that a mere violation of the right to the protection of personal data would not suffice since otherwise the third condition would become largely redundant.

52. Moreover, whether an imminent risk of such grave harm exists has to be assessed on the basis of the concrete situation of the complainant(s). As set out above, the conditions of Article 3 (1) (b) have to be met in the specific case at hand. However, the complainant has not brought forward any specific arguments which would indicate that there is an imminent risk of grave harm. Rather, due to their generality and abstractness, Mr Schrems' concerns about the surveillance programmes of the US national security agencies are exactly the same as those which have led the Commission to start the review the Safe Harbour Decision. National data protection authorities would encroach upon the Commission's competence to renegotiate the terms of the Safe Harbour Decision with the US or, if necessary, suspend the Decision if they took action based on complaints raising only structural and abstract concerns.

    This having been said, the Commission does not exclude that in other specific cases, where an imminent risk of grave harm to complainants is demonstrated, national data protection authorities could take action.

5.2.4. Fourth condition: The competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organization with notice and an opportunity to respond

53. As the third condition of Article 3 (1) (b) is not met, there is in principle no need to examine the fourth condition. However, should the Court come to a different result regarding the third condition, the Commission notes that it appears that the Commissioner did discuss the PRISM allegations with Facebook Ireland even before he had received Schrems' complaint and was satisfied with the responses provided including that the company "*had appropriate procedures in place for the handling of access requests received from security agencies generally*" (Appendix 1, submission on behalf of the respondent (Commissioner), point 66). From this, it could be concluded that the fourth condition was fulfilled. However, the Commission notes also that such discussions with the organization involved may not be sufficient to address problems created by the access to personal data by US national security agencies. This also supports the Commission's view that such issues are better addressed through review of the Safe Harbour Decision by the Commission.

5.3. No power of the data protection authority to investigate

54. If, as under circumstances such as in the main proceedings, not all of the cumulative conditions of Article 3 (1) (b) are met, the data protection authority has no power to investigate further a complaint. It is rather bound by the finding of adequacy by the Commission in the Safe Harbour Decision. This having been said, the Commission does not exclude that in other specific cases, where an imminent risk of grave harm to complainants is demonstrated national data protection authorities could take action.

6. CONCLUSION

55. In the light of the above observations, the Commission respectfully suggests that the Court should answer the questions referred for a preliminary ruling by the High Court of Ireland as follows:

Under circumstances such as in the main proceedings, the data protection authority is bound by the finding of adequacy by the European Commission in Decision 2000/520/EC (Safe Harbour Decision).

[redacted]

Ben Smulders Bernd Martenczuk Julie Vondung [redacted]

Agents for the Commission

Schedule of Annexes

Annex 1:

Report of the Findings by the EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection, 27.11.2013, referred to in paragraph 28 of the observations.

Annex 2:

Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU", COM(2013) 847, 27.11.2013, referred to in paragraph 29 of the observations.

Annex 3:

Communication from the Commission to the European Parliament and the Council, "Rebuilding Trust in EU-US Data Flows", COM(2013) 846, 27.11.2013, referred to in paragraphs 29 and 30 of the observations.

Date de réception : 23/01/2015

Published ID	:	C-362/14
Document number	:	13
Register number	:	976996
Date of lodgment	:	03/11/2014
Date of entry in the register	:	03/11/2014
Type of document	:	Observations
	:	Annexes Part 1
Lodgment reference	:	DC33346
File number	:	2
Person lodging document	:	Julie Vondung (R249125) Commission

Annex 1

Report of the Findings by the EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection, 27.11.2013, referred to in paragraph 28 of the observations.

Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection

27 November 2013

Report on the Findings of the EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection

1. AIM AND SETTING UP OF THE WORKING GROUP

In June 2013, the existence of a number of US surveillance programmes involving the large-scale collection and processing of personal data was revealed. The programmes concern in particular the collection of personal data from US internet and telecommunication service providers and the monitoring of data flows inside and outside the US. Given the central position of US information and communications technology companies in the EU market, the transatlantic routing of electronic data flows, and the volume of data flows across the Atlantic, significant numbers of individuals in the EU are potentially affected by the US programmes.

At the EU-US Justice and Home Affairs Ministerial Meeting in June 2013, and in letters to their US counterparts, Vice-President Reding and Commissioner Malmström expressed serious concerns regarding the impact of these programmes on the fundamental rights of individuals in the EU, particularly the fundamental right to protection of personal data. Clarifications were requested from the US authorities on a number of aspects, including the scope of the programmes, the volume of data collected, the existence of judicial and administrative oversight mechanisms and their availability to individuals in the EU, as well as the different levels of protection and procedural safeguards that apply to US and EU persons.

Further to a COREPER meeting of 18 July 2013, an ad hoc EU-US Working Group was established in July 2013 to examine these matters. The purpose was to establish the facts about US surveillance programmes and their impact on fundamental rights in the EU and personal data of EU citizens.

Further to that COREPER meeting, a "second track" was established under which Member States may discuss with the US authorities, in a bilateral format, matters related to their national security, and the EU institutions may raise with the US authorities questions related to the alleged surveillance of EU institutions and diplomatic missions.

On the EU side, the ad hoc Working Group is co-chaired by the Commission and the Presidency of the Council. It is composed of representatives of the Presidency, the Commission services, the European External Action Service, the incoming Presidency, the EU Counter-Terrorism Co-ordinator, the Chair of the Article 29 Working Party, as well as ten experts from Member States, having expertise in the area of data protection and law enforcement/security. On the US side, the group is composed of senior officials from the Department of Justice, the Office of the Director of National Intelligence, the State Department and the Department of Homeland Security.

A preparatory meeting took place in Washington, D.C. on 8 July 2013. Meetings of the Group took place on 22 and 23 July 2013 in Brussels, on 19 and 20 September 2013 in Washington, D.C., and on 6 November 2013 in Brussels.

The findings by the EU co-chairs of the ad hoc EU-US Working Group are presented in this report. The report is based on information provided by the US during the meetings of the ad hoc EU-US working group, as well as on publicly available documents, including classified documents disclosed in the press but not confirmed by the US. Participants on the EU side

had an opportunity to submit comments on the report. The US was provided with an opportunity to comment on possible inaccuracies in the draft. The final report has been prepared under the sole responsibility of the EU-co chairs.

The distinction between the EU-US Working Group and the bilateral second track, which reflects the division of competences between the EU and Member States and in particular the fact that national security remains the sole responsibility of each Member State, set some limitations on the discussion in the Working Group and the information provided therein. The scope of the discussions was also limited by operational necessities and the need to protect classified information, particularly information related to sources and methods. The US authorities dedicated substantial time and efforts to responding to the questions asked by the EU side on the legal and oversight framework in which their Signal Intelligence capabilities operate.

2. THE LEGAL FRAMEWORK

The US provided information regarding the legal basis upon which surveillance programmes are based and carried out. The US clarified that the President's authority to collect foreign intelligence outside the US derives directly from his capacity as "commander in chief" and from his competences for the conduct of the foreign policy, as enshrined in the US constitution.

The overall US constitutional framework, as interpreted by the US Supreme Court is also sufficiently relevant to make reference to it here. The protection of the Fourth Amendment of the US Constitution, which prohibits "unreasonable searches and seizures" and requires that a warrant must be based upon "probable cause"[1] extends only to US nationals and citizens of any nation residing within the US. According to the US Supreme Court, foreigners who have not previously developed significant voluntary connections with the US cannot invoke the Fourth Amendment[2].

Two legal authorities that serve as bases for the collection of personal data by US intelligence agencies are: Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA) (as amended by the 2008 FISA Amendments Act, 50 U.S.C. § 1881a); and Section 215 of the USA PATRIOT Act 2001 (which also amended FISA, 50 U.S.C. 1861). The FISA Court has a role in authorising and overseeing intelligence collection under both legal authorities.

The US further clarified that not all intelligence collection relies on these provisions of FISA; there are other provisions that may be used for intelligence collection. The Group's attention was also drawn to Executive Order 12333, issued by the US President in 1981 and amended most recently in 2008, which sets out certain powers and functions of the intelligence agencies, including the collection of foreign intelligence information. No judicial oversight is provided for intelligence collection under Executive Order 12333, but activities commenced pursuant to the Order must not violate the US constitution or applicable statutory law.

---

1 "Probable cause" must be shown before an arrest or search warrant may be issued. For probable cause to exist, there must be sufficient reason based upon known facts to believe a crime has been committed or that certain property is connected with a crime. In most cases, probable cause has to exist prior to arrest, search or seizure, including in cases when law enforcement authorities can make an arrest or search without a warrant.

2 According to the US Supreme Court, foreigners who are not residing permanently in the US can only rely on the Fourth Amendment if they are part of the US national community or have otherwise developed sufficient connection with the US to be considered part of that community: US v. Verdugo-Urquidez – 494 U.S. 259 (1990), pp. 494 U.S. 264-266.

2.1. Section 702 FISA (50 U.S.C. § 1881a)

2.1.1. Material scope of Section 702 FISA

Section 702 FISA provides a legal basis for the collection of "foreign intelligence information" regarding persons who are "reasonably believed to be located outside the United States." As the provision is directed at the collection of information concerning non-US persons, it is of particular relevance for an assessment of the impact of US surveillance programmes on the protection of personal data of EU citizens.

Under Section 702, information is obtained "from or with the assistance of an electronic communication service provider". This can encompass different forms of personal information (e.g. emails, photographs, audio and video calls and messages, documents and internet browsing history) and collection methods, including wiretaps and other forms of interception of electronically stored data and data in transmission.

The US confirmed that it is under Section 702 that the National Security Agency (NSA) maintains a database known as PRISM. This allows collection of electronically stored data, including content data, by means of directives addressed to the main US internet service providers and technology companies providing online services, including, according to classified documents disclosed in the press but not confirmed by the US, Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Apple, Skype and YouTube.

The US also confirmed that Section 702 provides the legal basis for so-called "upstream collection"; this is understood to be the interception of Internet communications by the NSA as they transit through the US [3] (e.g. through cables, at transmission points).

Section 702 does not require the government to identify particular targets or give the Foreign Intelligence Surveillance Court (hereafter 'FISC') Court a rationale for individual targeting. Section 702 states that a specific warrant for each target is not necessary.

The US stated that no blanket or bulk collection of data is carried out under Section 702, because collection of data takes place only for a specified foreign intelligence purpose. The actual scope of this limitation remains unclear as the concept of foreign intelligence has only been explained in the abstract terms set out hereafter and it remains unclear for exactly which purposes foreign intelligence is collected. The EU side asked for further specification of what is covered under "foreign intelligence information," within the meaning of FISA 50, U.S.C. §1801(e), such as references to legal authorities or internal guidelines substantiating the scope of foreign intelligence information and any limitations on its interpretation, but the US explained that they could not provide this as to do so would reveal specific operational aspects of intelligence collection programmes. "Foreign intelligence information", as defined by FISA, includes specific categories of information (e.g. international terrorism and international proliferation of weapons of mass destruction) as well as "information relating to the conduct of the foreign affairs of the US." Priorities are identified by the White House and the Director of National Intelligence and a list is drawn up on the basis of these priorities.

Foreign intelligence could, on the face of the provision, include information concerning the political activities of individuals or groups, or activities of government agencies, where such activity could be of interest to the US for its foreign policy[4]. The US noted that "foreign

---

[3] Opinions of the Foreign Intelligence Surveillance Court (FISC) of 3 October 2011 and of 30 November 2011.

[4] 50 U.S.C. §1801(e) (2) read in conjunction with §1801(a) (5) and (6).

intelligence" includes information gathered with respect to a foreign power or a foreign territory as defined by FISA, 50 USC 1801.

On the question whether "foreign intelligence information" can include activities that could be relevant to US economic interests, the US stated that it is not conducting any form of industrial espionage and referred to statements of the President of the United States[5] and the Director of National Intelligence[6]. The US explained that it may collect economic intelligence (e.g. the macroeconomic situation in a particular country, disruptive technologies) that has a foreign intelligence value. However, the US underlined that information that is obtained which may provide a competitive advantage to US companies is not authorised to be passed on to those companies.

Section 702 provides that upon issuance of an order by the FISC, the Attorney General and the Director of National Intelligence may authorize jointly the targeting of persons reasonably believed to be located outside the US to acquire foreign intelligence information. Section 702 does not require that foreign intelligence information be the sole purpose or even the primary purpose of acquisition, but rather "a significant purpose of the acquisition". There can be other purposes of collection in addition to foreign intelligence. However, the declassified FISC Opinions indicate that, due to the broad method of collection applied under the upstream programme and also due to technical reasons, personal data is collected that may not be relevant to foreign intelligence[7].

2.1.2. Personal scope of Section 702 FISA

Section 702 FISA governs the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information". It is aimed at the targeting of non-US persons who are overseas.

This is confirmed by the limitations set forth in Section 702 (b) FISA which exclusively concern US citizens or non-US persons within the US[8]. More specifically, acquisition of data authorised under Section 702 may not:

---

5 Speaking at a press conference in Stockholm on 4 September 2013, President Obama said: "when it comes to intelligence gathering internationally, our focus is on counterterrorism, weapons of mass destruction, cybersecurity -- core national security interests of the United States".

6 Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage, 8 September 2013: "What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of - or give intelligence we collect to - US companies to enhance their international competitiveness or increase their bottom line"; full statement available at: http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations-of-economic-espionage.

7 According to the FISC Declassified Opinion of 3 October 2011, "NSAs 'upstream collection' of Internet communications includes the acquisition of entire 'transactions'", which "may contain data that is wholly unrelated to the tasked selector, including the full content of discrete communications that are not to, from, or about the facility tasked for collection" (p. 5). The FISC further notes that "NSA's upstream collection devices have technological limitations that significantly affect the scope of collection" (p. 30), and that "NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from or about a tasked selector" (p. 31). It is stated in the FISC Declassified Opinion that "the portions of MCTs [multi communication transactions] that contain references to targeted selectors are likely to contain foreign intelligence information, and that it is not feasible for NSA to limit its collection only to the relevant portion or portions of each MCT" (p. 57).

8 "US person" is defined in 50 U.S.C. §1801(i) as a US citizen, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are US citizens or

(i) intentionally target any person known at the time of acquisition to be located in the US;

(ii) intentionally target a person believed to be located outside the US if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the US;

(iii) intentionally target a US person reasonably believed to be located outside the US;

(iv) intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the US.

In addition, pursuant to the same provision, acquisition of data must be "conducted in a manner consistent with the Fourth Amendment to the Constitution of the United States", that prohibits "unreasonable searches and seizures" and requires that a warrant must be based upon "probable cause".

As far as US persons are concerned, the definition of "foreign intelligence information" requires that the information to be collected is *necessary* to the purpose pursued[9]. Concerning non-US persons, the definition of "foreign intelligence information" only requires the information to be *related* to the purpose pursued[10].

As discussed below, collection under Section 702 is subject to targeting and minimisation procedures that aim to reduce the collection of personal data of US persons under Section 702, as well as the further processing of personal data of US persons incidentally acquired under Section 702. While, according to the US, non US persons may benefit from some requirements set out in the minimization procedures[11], there are no targeting or minimisation procedures under Section 702 that specifically aim to reduce the collection and further processing of personal data of non-US persons incidentally acquired.

2.1.3. Geographical scope of Section 702 FISA

Section 702 does not contain limitations on the geographical scope of collection of foreign intelligence information.

Section 702 (h) provides that the Attorney General and the Director of National Intelligence may direct an "electronic communication service provider" to provide immediately all information, facilities or assistance necessary. This encompasses a wide range of electronic communication services and operators, including those that may have personal data pertaining to individuals in the EU in their possession:

(i) any service which provides users with the ability to send or receive wire or electronic communications (this could include e.g. email, chat and VOIP providers)[12];

(ii) any "remote computing" service, i.e. one which provides to the public computer storage or processing services by means of an electronic communications system[13];

(iii) any provider of telecommunications services (e.g. Internet service providers)[14]; and

(iv) any other communication service provider who has access to wire or electronic communications either as they are transmitted or as they are stored[15].

---

permanent residents, or a corporation incorporated in the US but not including a corporation or association that is a foreign power.

9 50 U.S.C. §1801(e).

10 Ibid.

11 Declassified minimization procedures (2011) used by the NSA in connection with acquisitions of foreign intelligence information pursuant to Section 702 FISA. See Section 3 (a)

12 FISA s.701 (b)(4)(B); 18 U.S.C. § 2510.

13 FISA s.701 (b) (4) (C); 18 U.S.C. § 2711.

14 FISA s.701 (b) (4) (A); 47 U.S.C. § 153.

Declassified FISC opinions confirm that US intelligence agencies have recourse to methods of collection under Section 702 that have a wide reach, such as the PRISM collection of data from internet service providers or through the "upstream collection" of data that transits through the US[16].

The EU asked for specific clarifications on the issue of collection of or access to data not located or not exclusively located in the US; data stored or otherwise processed in the cloud; data processed by subsidiaries of US companies located in the EU; and data from Internet transmission cables outside the US. The US declined to reply on the grounds that the questions pertained to methods of intelligence collection.

2.2. Section 215 US Patriot Act (50 U.S.C. § 1861)

Section 215 of the USA-Patriot Act 2001 is the second legal authority for surveillance programmes that was discussed by the ad hoc EU-US working group. It permits the Federal Bureau of Investigation (FBI) to make an application for a court order requiring a business or another entity to produce "tangible things", such as books, records or documents, where the information sought is relevant for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities[17]. The order is secret and may not be disclosed. However, the US Office of the Director of National Intelligence declassified and made public some documents related to Section 215, including documents revealing the legal reasoning of the FISC on Section 215.

The US confirmed that this provision serves as the basis for a programme of intelligence collection via orders obtained by the FBI from the FISC directing certain telecommunications service providers to provide specified non-content telephony "meta-data". For that programme, the information is stored by the NSA and queried only for counter-terrorism purposes.

That programme is limited to the collection of call detail records, or telephony "meta-data" maintained by specified telecommunications service providers. These records cover information such as telephone numbers dialled and the numbers from which calls are made, as well as the date, time and duration of calls, but do not include the content of the calls, the names, address or financial information of any subscriber or customer, or any cell site location information. According to the explanations provided by the US, this means that the intelligence agencies cannot, through this programme, listen to or record telephone conversations.

The US explained that Section 215 allows for "bulk" collection of telephony meta-data maintained by the company to whom the order is addressed. The US also explained that, although the collection is broad in scope, the further processing of the meta-data acquired under this programme is limited to the purpose of investigation of international terrorism. It was stated that the bulk records may not be accessed or queried by intelligence agencies for any other purpose.

An order for data under Section 215 can concern not only the data of US persons, but also of non-US persons. Both US and EU data subjects, wherever located, fall within the scope of the

---

15 FISA s.701 (b) (4) (D).

16 See declassified letters of 4 May 2002 from DOJ and ODNI to the Chairman of the US senate and House of Representatives' Select Committee on Intelligence, p. 3-4 of annexed document.

17 Section 215 further specifies that production of information can relate to an investigation on international terrorism or clandestine intelligence activities concerning a US person, provided that such investigation of a US person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

telephony meta-data programme, whenever they are party to a telephone call made to, from or within the US and whose meta-data is maintained and produced by a company to whom the order is addressed.

There are limitations on the scope of Section 215 generally: when applying for an order, the FBI must specify reasonable grounds to believe that the records sought are relevant to an authorised investigation to obtain foreign intelligence information not concerning a US person, or to protect against international terrorism or clandestine intelligence activities. In addition, US persons benefit under Section 215 from a further protection unavailable to non-US persons, as Section 215 specifically excludes from its scope "investigation of a United States person [...] conducted solely upon the basis of activities protected by the first amendment to the Constitution", i.e. activities protected by the freedom of religion, the freedom of speech or of the press, as well as the freedom of assembly and to petition the Government for redress for grievances.

2.3. Executive Order 12333

The US indicated that Executive Order 12333 serves as the basis for other surveillance programmes, the scope of which is at the discretion of the President. The US confirmed that Executive Order 12333 is the general framework on intelligence gathering inside and outside the US. Although the Executive Order requires that agencies operate under guidelines approved by the head of the agency and the Attorney General, the Order itself does not set any restriction to bulk collection of data located outside the US except to reiterate that all intelligence collection must comply with the US Constitution and applicable law. Executive Order 12333 also provides a legal basis to disseminate to foreign governments information acquired pursuant to Section 702[18].

The EU requested further information regarding the scope and functioning of Executive Order 12333 and the guidelines and supplemental procedures whose adoption is provided for under the Executive Order. The EU requested information in particular with regard to the application of Executive Order 12333 to bulk data collection, its impact on individuals in the EU and any applicable safeguards. The US explained that the part that covers signals intelligence annexed to the relevant regulation setting forth procedures under Executive Order 12333 is classified, as are the supplementary procedures on data analysis, but that the focus of these procedures is on protecting information of US persons. The US indicated that the limitations on intelligence collection under Executive Order 12333 are not designed to limit the collection of personal data of non-US persons. For example, on the question whether collection of inbox displays from email accounts and/or collection of contact lists are authorised, the US representatives replied that they were not aware of a prohibition of such practices.

The US confirmed that judicial approval is not required under Executive Order 12333 and that there is no judicial oversight of its use, except in limited circumstances such as when information is used in a legal proceeding. Executive oversight is exercised under Executive Order 12333 by the Inspector-Generals of each agency, who regularly report to the heads of their agencies and to Congress on the use as well as on breaches of Executive Order 12333. The US was unable to provide any quantitative information with regard to the use or impact on EU citizens of Executive Order 12333. The US did explain, however, that the Executive Order states that intelligence agencies should give "special emphasis" to detecting and

[18] See Declassified minimization procedures, at p. 11.

countering the threats posed by terrorism, espionage, and the proliferation of weapons of mass destruction[19].

The US further confirmed that in the US there are other legal bases for intelligence collection where the data of non-US persons may be acquired but did not go into details as to the legal authorities and procedures applicable.

3. COLLECTION AND FURTHER PROCESSING OF DATA

In response to questions from the EU regarding how data is collected and used under the surveillance programmes, the US stated that the collection of personal information based on Section 702 FISA and Section 215 Patriot Act is subject to a number of procedural safeguards and limitative conditions. Under both legal authorities, according to the US, privacy is protected by a multi-layered system of controls on what is collected and on the use of what is collected, and these controls are based on the nature and intrusiveness of the collection.

It appeared from the discussions that there is a significant difference in interpretation between the EU and the US of a fundamental concept relating to the processing of personal data by security agencies. For the EU, data acquisition is synonymous with data collection and is a form of processing of personal data. Data protection rights and obligations are already applicable at that stage. Any subsequent operation carried out on the data collected, such as storage or consultation by human eyes, constitutes further processing. As the US explained, under US law, the initial acquisition of personal data does not always constitute processing of personal data; data is "processed" only when it is analysed by means of human intervention. This means that while certain safeguards arise at that moment of acquisition, additional data protection safeguards arise at the time of processing.

3.1. Section 702 FISA

3.1.1. Certification and authorization procedure

Section 702 does not require individual judicial orders or warrants authorizing collection against each target. Instead, the FISC approves annual certifications submitted in writing by the Attorney General and the Director of National Intelligence. Both the certifications and the FISC's orders are secret, unless declassified under US law. The certifications, which are renewable, identify categories of foreign intelligence information sought to be acquired. They are therefore critical documents for a correct understanding of the scope and reach of collection pursuant to Section 702.

The EU requested, but did not receive, further information regarding how the certifications or categories of foreign intelligence purposes are defined and is therefore not in a position to assess their scope. The US explained that the specific purpose of acquisition is set out in the certification, but was not in a position to provide members of the Group with examples because the certifications are classified. The FISC has jurisdiction to review certifications as well as targeting and minimization procedures. It reviews Section 702 certification to ensure that they contain all required elements and targeting and minimization procedures to ensure that they are consistent with FISA and the Fourth Amendment to the US Constitution. The certification submitted to the FISC by the Attorney General and the Director of National Intelligence must contain all the required elements under Section 702 (i), including an attestation that a significant purpose of the acquisition is to obtain foreign intelligence information. The FISC does not scrutinise the substance of the attestation or the need to acquire data against the purpose of the acquisition, e.g. whether it is consistent with the

[19] See Executive Order 12333, Part 1.1 (c).

purpose or proportionate, and in this regard cannot substitute the determination made by the Attorney General and the Director of National Intelligence. Section 702 expressly specifies that certifications are not required to identify the specific facilities, places, premises, or property to which an acquisition of data will be directed or in which it will be conducted.

On the basis of FISC-approved certifications, data is collected by means of directives addressed to electronic communications services providers to provide any and all assistance necessary. On the question of whether data is "pushed" by the companies or "pulled" by the NSA directly from their infrastructure, the US explained that the technical modalities depend on the provider and the system they have in place; providers are supplied with a written directive, respond to it and are therefore informed of a request for data. There is no court approval or review of the acquisition of data in each specific case.

According to the US,[20] under Section 702, once communications from specific targets that are assessed to possess, or that are likely to communicate, foreign intelligence information have been acquired, the communications may be queried. This is achieved by tasking selectors that are used by the targeted individual, such as a telephone number or an email address. The US explained that there are no random searches of data collected under Section 702, but only targeted queries. Query terms include names, email addresses, telephone numbers, or keywords. When query terms are used to search databases, there is no requirement of reasonable suspicion neither of unlawful activity nor of a specific investigation. The applicable criterion is that the query terms should be reasonably believed to be used to return foreign intelligence information. The US confirmed that it is possible to perform full-text searches of communications collected, and access both content information and metadata with respect to communications collected.

The targeting decisions made by NSA in order to first acquire communications are reviewed after-the-fact by the Department of Justice and the Office of the Director of National Intelligence; other instances of oversight exist within the executive branch. There is no judicial scrutiny of the selectors tasked, e.g. their reasonableness or their use. The EU requested further information on the criteria on the basis of which selectors are defined and chosen, as well as examples of selectors, but no further clarifications were provided.

The collection of data is subject to specific "minimisation" procedures approved by the FISC. These procedures explicitly apply to information incidentally collected of, or concerning, US persons. They primarily aim to protect the privacy rights of US persons, by limiting the collection, retention, and dissemination of incidentally acquired information to, from or about US persons. There is no obligation to minimize impact on non-US persons outside the US. However, according to the US, the minimisation procedures also benefit non-US persons, since they are aimed at limiting the collection to data reasonably relevant to a foreign intelligence purpose[21]. An example provided by the US is in Section 4 of the Minimisation Procedures, which contains attorney-client protections for anyone under indictment in the United States, regardless of citizenship status.

---

[20] See also Semi-Annual Assessment of Compliance with the Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, declassified by the Director of National Intelligence on 21 August 2013(http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf), Annex A, p. A2.

[21] Ibid, at p. 4, Section 3 (b) (4); but see also the declassified November 2011 FISC Opinion which found that measures previously proposed by the government to comply with this requirement had been found to be unsatisfactory in relation to "upstream" collection and processing; and that new measures were only found to be satisfactory for the protection of US persons.

The collection of data is also subject to specific "targeting" procedures that are approved by the FISC. These "targeting" procedures primarily aim to protect the privacy rights of US persons, by ensuring that, in principle, only non-US persons located abroad are targeted. However, the US refers to the fact that the targeting procedures contain factors for the purpose of assessing whether a target possesses and/or is likely to communicate foreign intelligence information[22].

The US did not clarify whether and how other elements of the minimisation and targeting procedures apply in practice to non-US persons, and did not state which rules apply in practice to the collection or processing of non-US personal data when it is not necessary or relevant to foreign intelligence. For example, the EU asked whether information that is not relevant but incidentally acquired by the US is deleted and whether there are guidelines to this end. The US was unable to provide a reply covering all possible scenarios and stated that the retention period would depend on the applicable legal basis and certification approved by FISC.

Finally, the FISC review does not include review of potential measures to protect the personal information of non-US persons outside the US.

3.1.2. Quantitative indicators

In order to assess the reach of the surveillance programmes under Section 702 and in particular their impact on individuals in the EU, the EU side requested figures, e.g. how many certifications and selectors are currently used, how many of them concern individuals in the EU, or regarding the storage capacities of the surveillance programmes. The US did not discuss the specific number of certification or selectors. Additionally, the US was unable to quantify the number of individuals in the EU affected by the programmes.

The US confirmed that 1.6% of all global internet traffic is "acquired" and 0.025% of it is selected for review; hence 0.0004% of all global internet traffic is looked at by NSA analysts. The vast majority of global internet traffic consists of high-volume streaming and downloads such as television series, films and sports[23]. Communications data makes up a very small part of global internet traffic. The US did not confirm whether these figures included "upstream" data collection.

3.1.3. Retention Periods

The US side explained that "unreviewed data" collected under Section 702 is generally retained for five years, although data collected via upstream collection is retained for two years. The minimisation procedures only state these time limits in relation to US-persons data[24]. However, the US explained that these retention periods apply to all unreviewed data, so they apply to both US and non-US person information.

---

22 See declassified NSA targeting procedures, p 4.

23 See Cisco Visual Networking Index, 2012 (available at: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf)

24 See Declassified minimisation procedures, at p.11, Section 7; and the declassified November 2011 FISC Opinion, at page 13-14: "The two-year period gives NSA substantial time to review its upstream acquisitions for foreign intelligence information but ensures that non-target information that is subject to protection under FISA or the Fourth Amendment [i.e. information pertaining to US persons] is not retained any longer than is reasonably necessary... the Court concludes that the amended NSA minimization procedures, as NSA is applying them to ["upstream collection" of Internet transactions containing multiple communications], are "reasonably designed ... to minimize the ... retention[] ... of non-publicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."

If the data is deemed to be of foreign intelligence interest, there is no limitation on the length of retention. The US did not specify the retention period of data collected under Executive Order 12333.

The EU asked what happens to "non-responsive" information (i.e. data collected that does not respond to query on the basis of a query term). The US responded that it is not "collecting" non-responsive information. According to the US, information that is not reviewed pursuant to a query made to that database normally will "age off of the system". It remains unclear whether and when such data is deleted.

3.1.4. Onward transfers and sharing of information

The US indicated that the collected data are stored in a secure database with limited access for authorised staff only. The US however also confirmed that in case data collected under Section 702 reveal indications of criminal conduct, they can be transferred to or shared with other agencies outside the intelligence community, e.g. law enforcement agencies, for purposes other than foreign intelligence and with third countries. The minimisation procedures of the recipient agency are applicable. "Incidentally obtained" information (information not relevant to foreign intelligence) may also be shared if such information meets the standard under the applicable procedures.

On the use of private contractors, the US insisted that all contractors are vetted and subject to the same rules as employees.

3.1.5. Effectiveness and added value

The US stated that in 54 instances, collection under Sections 702 and 215 contributed to the prevention and combating of terrorism; 25 of these involved EU Member States. The US was unable to provide figures regarding Executive Order 12333. The US confirmed that out of the total of 54 cases, 42 cases concerned plots that were foiled or disrupted and 12 cases concerned material support for terrorism cases.

3.1.6. Transparency and remedies ex-post

The EU asked whether people who are subject to surveillance are informed afterwards, where such surveillance turns out to be unjustified. The US stated that such a right does not exist under US law. However, if information obtained through surveillance programmes is subsequently used for the purposes of criminal proceedings, the protections available under US criminal procedural law apply.

3.1.7. Overarching limits on strategic surveillance of data flows

The EU asked whether surveillance of communications of people with no identified link to serious crime or matters of state security is limited, for example in terms of quantitative limits on the percentage of communications that can be subject to surveillance. The US stated that no such limits exist under US law.

3.2. Section 215 US Patriot Act

3.2.1. Authorization procedure

Under the Section 215 programme discussed herein, the FBI obtains orders from the FISC directing telecommunications service providers to provide telephony meta-data. The US explained that, generally, the application for an order from the FISC pursuant to Section 215 must specify reasonable grounds to believe that the records are relevant to an authorised investigation to obtain foreign intelligence information not concerning a US person or to protect against international terrorism or clandestine intelligence activities. Under the telephony metadata collection programme, the NSA, in turn, stores and analyses these bulk

records which can be queried only for counterterrorism purposes. The US explained that the information sought must be "relevant" to an investigation and that this is understood broadly, since a piece of information that might not be relevant at the time of acquisition could subsequently prove to be relevant for an investigation. The standard applied is less stringent than "probable cause" under criminal law and permits broad collection of data in order to allow the intelligence authorities to extract relevant information.

The legal standard of relevance under Section 215 is interpreted as not requiring a separate showing that every individual record in the database is relevant to the investigation. It appears that the standard of relevance is met if the entire database is considered relevant for the purposes sought.[25] While FISC authorization is not required prior to the searching of the data by the NSA, the US stated that Court has approved the procedures governing access to the meta-data acquired and stored under the telephony meta-data programme authorised under Section 215. A small number of senior NSA officials have been authorised to determine whether the search of the database meets the applicable legal standard. Specifically, there must be a "reasonable, articulable suspicion" that an identifier (e.g. a telephone number) used to query the meta-data is associated with a specific foreign terrorist organisation. It was explained by the US that the "reasonable, articulable suspicion" standard constitutes a safeguard against the indiscriminate querying of the collected data and greatly limits the volume of data actually queried.

The US also stressed that they consider that constitutional privacy protections do not apply to the type of data collected under the telephony meta-data programme. The US referred to case-law of the US Supreme Court[26] according to which parties to telephone calls have no reasonable expectation of privacy for purposes of the Fourth Amendment regarding the telephone numbers used to make and receive calls; therefore, the collection of meta-data under Section 215 does not affect the constitutional protection of privacy of US persons under the Fourth Amendment.

3.2.2. Quantitative indicators

The US explained that only a very small fraction of the telephony meta-data collected and retained under the Section 215-authorised programme is further reviewed, because the vast majority of the data will never be responsive to a terrorism-related query. It was further explained that in 2012 less than 300 unique identifiers were approved as meeting the "reasonable, articulable suspicion" standard and were queried. According to the US, the same identifier can be queried more than once, can generate multiple responsive records, and can be used to obtain second and third-tier contacts of the identifier (known as "hops"). The actual number of queries can be higher than 300 because multiple queries may be performed using the same identifier. The number of persons affected by searches on the basis of these identifiers, up to third-tier contacts, remains therefore unclear.

In response to the question of the quantitative impact of the Section 215 telephony meta-data programme in the EU, for example how many EU telephone numbers calling into the US or having been called from the US have been stored under Section 215-authorised programmes, the US explained that it was not able to provide such clarifications because it does not keep this type of statistical information for either US or non-US persons.

---

[25] See letter from DOJ to Representative Sensenbrenner of 16 July 2013 (http://beta.congress.gov/congressional-record/2013/7/24/senate-section/article/H5002-1)

[26] U.S. Supreme Court, *Smith v. Maryland*, 442 U.S. 735 (1979):

3.2.3. Retention periods

The US explained that, in principle, data collected under Section 215 is retained for five years, with the exception for data that are responsive to authorized queries. In regard to data that are responsive to authorized queries, the data may be retained pursuant to the procedures of the agency holding the information, e.g. the NSA or another agency such as the FBI with whom NSA shared the data. The US referred the Group to the "Attorney General's Guidelines for Domestic FBI Operations"[27] which apply to data that is further processed in a specific investigation. These Guidelines do not specify retention periods but provide that information obtained will be kept in accordance with a records retention plan approved by the National Archives and Records Administration. The National Archives and Records Administration's General Records Schedules do not establish specific retention periods that would be appropriate to all applications. Instead, it is provided that electronic records should be deleted or destroyed when "the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes".[28] It follows that the retention period for data processed in a specific investigation is determined by the agency holding the information or conducting the investigation.

3.2.4. Onward transfers and sharing of information

The EU asked for details with regards to sharing of data collected under Section 215 between different agencies and for different purposes. According to the US, the orders for the production of telephony meta-data, among other requirements, prohibit the sharing of the raw data and permit NSA to share with other agencies only data that are responsive to authorized queries for counterterrorism queries. In regard to the FBI's handling of data that it may receive from the NSA, the US referred to the "Attorney General's Guidelines for Domestic FBI Operations"[29]. Under these guidelines, the FBI may disseminate collected personal information to other US intelligence agencies as well as to law enforcement authorities of the executive branch (e.g. Department of Justice) for a number of reasons or on the basis of other statutes and legal authorities[30].

4. OVERSIGHT AND REDRESS MECHANISMS

The US explained that activities authorised by Section 702 FISA and Section 215 Patriot Act are subject to oversight by the executive, legislative and judicial branches.

The oversight regime and the balance between the roles of each of the branches in overseeing the surveillance programmes differ according to the legal basis of collection. For instance, because judicial oversight is limited in relation to Section 702 and collection under Executive Order 12333 is not subject to judicial oversight, a greater role is played by the executive

---

27 Available at: http://www.justice.gov/ag/readingroom/guidelines.pdf, p. 35.

28 Available at: http://www.archives.gov/records-mgmt/grs/grs20.html: "The records covered by several items in this schedule are authorized for erasure or deletion when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes. NARA cannot establish a more specific retention that would be appropriate in all applications. Each agency should, when appropriate, determine a more specific disposition instruction, such as "Delete after X update cycles" or "Delete when X years old," for inclusion in its records disposition directives or manual. NARA approval is not needed to set retention periods for records in the GRS that are authorized for destruction when no longer needed."

29 Available at: http://www.justice.gov/ag/readingroom/guidelines.pdf.

30 Attorney General's Guidelines for Domestic FBI Operations, p. 35-36, provide that "[t]he FBI shall share and disseminate information as required by statutes, treaties, Executive Orders, Presidential directives, National Security Council directives, Homeland Security Council directives, and Attorney General-approved policies, memoranda of understanding, or agreements".

branch in these cases. Oversight regarding whether collection on a foreign target is in keeping with Section 702 would appear to take place largely with the Department of Justice and the Office of the Director of National Intelligence as the responsible departments of the executive branch.

4.1. Executive oversight

Executive Branch oversight plays a role both prior to the collection of intelligence and following the collection, with regard to the processing of the intelligence. The National Security Division of the Department of Justice oversees the implementation of its decisions on behalf of the US intelligence community. These attorneys, together with personnel from the Office of the Director of National Intelligence, review each tasking under FISA 702 (checking justification for a valid foreign intelligence purpose; addressing over-collection issues, ensuring that incidents are reported to the FISC) and the request for production under Section 215 Patriot Act. The Department of Justice and the Office of the Director of National Intelligence also submit reports to Congress on a twice-yearly basis and participates in regular briefings to the intelligence committees of both the House of Representatives and the Senate to discuss FISA-related matters.

Once the data is collected, a number of executive oversight mechanisms and reporting procedures apply. There are internal audits and oversight controls (e.g. the NSA employs more than 300 personnel who support compliance efforts). Each of the 17 agencies that form the intelligence community, including the Office of the Director of National Intelligence have a General Counsel and an Inspector General. The independence of certain Inspectors General is protected by a statute and who can review the operation of the programmes, compel the production of documents, carry out on-site inspections and address Congress when needed. Regular reporting is done by the executive branch and submitted to the FISC and Congress.

As an example, the NSA Inspector-General in a letter of September 2013 to Congress referred to twelve compliance incidents related to surveillance under Executive Order 12333.In this context, the US drew the Group's attention to the fact that since 1 January 2003 nine individuals have been investigated in relation to the acquisition of data related to non-US persons for personal interests. The US explained that these employees either retired, resigned or were disciplined.

There are also layers of external oversight within the Executive Branch by the Department of Justice, the Director of National Intelligence and the Privacy and Civil Liberties Oversight Board.

The Director of National Intelligence plays an important role in the definition of the priorities which the intelligence agencies must comply with. The Director of National Intelligence also has a Civil Liberties Protection Officer who reports directly to the Director.

The Privacy and Civil Liberties Oversight Board was established after 9/11. It is comprised of four part-time members and a full-time chairman. It has a mandate to review the action of the executive branch in matters of counterterrorism and to ensure that civil liberties are properly balanced. It has investigation powers, including the ability to access classified information.

While the US side provided a detailed description of the oversight architecture,[31] the US did not provide qualitative information on the depth and intensity of oversight or answers to all questions about how such mechanisms apply to non-US persons.

---

[31] See Semi-Annual Assessment of Compliance.

4.2. Congressional oversight

Congressional oversight of intelligence activities is conducted through the Intelligence Committee and the Judiciary Committee of both Senate and the House, which employ approximately 30 to 40 staff. The US emphasised that both Committees are briefed on a regular basis, including on significant FISC opinions authorising intelligence collection programmes, and that there was specific re-authorisation of the applicable laws by Congress, including the bulk collection under Section 215 Patriot Act [32].

4.3. Judicial oversight: FISC role and limitations

The FISC, comprised of eleven Federal judges, oversees intelligence activities that take place on the basis of Section 702 FISA and Section 215 Patriot Act. Its proceedings are *in camera* and its orders and opinions are classified, unless they are declassified. The FISC is presented with government requests for surveillance in the form of authorisations for collection or certifications, which can be approved, sent back for improvement, e.g. to be modified or narrowed down, or refused. The number of formal refusals is very small. The US explained that the reason for this is the amount of scrutiny of these requests by different layers of administrative control before reaching the FISC, as well as the iterative process between the FISC and the administration prior to a FISC decision. According to the US, FISC has estimated that at times approximately 25% of applications submitted are returned for supplementation or modification.

What exactly is subject to judicial oversight depends on the legal basis of collection. Under Section 215, the Court is asked to approve collection in the form of an order to a specified company for production of records. Under Section 702, it is the Attorney General and the Director of National Intelligence that authorise collection, and the Court's role consists of confirmation that the certifications submitted contain all the elements required and that the procedures are consistent with the statute. There is no judicial oversight of programmes conducted under Executive Order 12333.

The limited information available to the Working Group did not allow it to assess the scope and depth of oversight regarding the impact on individuals in the EU. As the limitations on collection and processing apply primarily to US persons as required by the US Constitution, it appears that judicial oversight is limited as far as the collection and further processing of the personal data of non-US persons are concerned.

Under Section 702, the FISC does not approve government-issued directives addressed to companies to assist the government in data collection, but the companies can nevertheless bring a challenge to a directive in the FISC. A decision of the FISC to modify, set aside or enforce a directive can be appealed before the FISA Court of Review. Companies may contest directives on grounds of procedure or practical effects (e.g. disproportionate burden or departure from previous orders). It is not possible for a company to mount a challenge on the substance as the reasoning of the request is not provided.

FISC proceedings are non-adversarial and there is no representation before the Court of the interests of the data subject during the consideration of an application for an order. In addition, the US Supreme Court has established that individuals or organisations do not have standing to bring a lawsuit under Section 702, because they cannot know whether they have been subject to surveillance or not[33]. This reasoning would apply to both US and EU data

---

[32] In addition, the Congressional committees are provided with information from the FISC regarding its procedures and working methods; see, for example, the letters of FISA Court Presiding Judge Reggie Walton to Senator Leahy of 29 July 2013 and 11 October 2013.

[33] *Clapper v Amnesty International*, Judgment of 26 February 2013, 568 U. S. (2013)

subjects. In light of the above, it appears that individuals have no avenues for judicial redress under Section 702 of FISA.

5. SUMMARY OF MAIN FINDINGS

(1) Under US law, a number of legal bases allow large-scale collection and processing, for foreign intelligence purposes, including counter-terrorism, of personal data that has been transferred to the US or is processed by US companies. The US has confirmed the existence and the main elements of certain aspects of these programmes, under which data collection and processing is done with a basis in US law that lays down specific conditions and safeguards. Other elements remain unclear, including the number of EU citizens affected by these surveillance programmes and the geographical scope of surveillance programmes under Section 702.

(2) There are differences in the safeguards applicable to EU data subjects compared to US data subjects, namely:

i. Collection of data pertaining to US persons is, in principle, not authorised under Section 702. Where it is authorised, data of US persons is considered to be "foreign intelligence" only if *necessary* to the specified purpose. This necessity requirement does not apply to data of EU citizens which is considered to be "foreign intelligence" if it *relates* to the purposes pursued. This results in lower threshold being applied for the collection of personal data of EU citizens.

ii. The targeting and minimisation procedures approved by FISC under Section 702 are aimed at reducing the collection, retention and dissemination of personal data of or concerning US persons. These procedures do not impose specific requirements or restrictions with regard to the collection, processing or retention of personal data of individuals in the EU, even when they have no connection with terrorism, crime or any other unlawful or dangerous activity. Oversight of the surveillance programmes aims primarily at protecting US persons.

iii. Under both Section 215 and Section 702, US persons benefit from constitutional protections (respectively, First and Fourth Amendments) that do not apply to EU citizens not residing in the US.

(3) Moreover, under US surveillance programmes, different levels_of data protection safeguards apply to different types of data (meta-data vs. content data) and different stages of data processing (initial acquisition vs. further processing/analysis).

(4) A lack of clarity remains as to the use of other available legal bases, the existence of other surveillance programmes as well as limitative conditions applicable to these programmes. This is especially relevant regarding Executive Order 12333.

(5) Since the orders of the FISC are classified and companies are required to maintain secrecy with regard to the assistance they are required to provide, there are no avenues, judicial or administrative, for either EU or US data subjects to be informed of whether their personal data is being collected or further processed. There are no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress.

(6) Various layers of oversight by the three branches of Government apply to activities on the base of Section 215 and Section 702. There is judicial oversight for activities that imply a capacity to compel information, including FISC orders for the collection under Section 215 and annual certifications that provide the basis for collection under Section 702. There is no judicial approval of individual selectors to query the data collected under Section 215 or tasked for collection under Section 702. The FISC operates *ex parte* and *in camera*. Its orders and opinions are classified, unless they are declassified. There is no judicial oversight of the collection of foreign intelligence outside the US under Executive Order 12333, which are conducted under the sole competence of the Executive Branch.

ANNEX: LETTERS OF VICE-PRESIDENT VIVIANE REDING, COMMISSIONER FOR JUSTICE, FUNDAMENTAL RIGHTS AND CITIZENSHIP AND COMMISSIONER CECILIA MALMSTRÖM, COMMISSIONER FOR HOME AFFAIRS, TO US COUNTERPARTS

Ref. Ares(2013)1935546 - 10/06/2013

European Commission

Viviane REDING
Vice-President of the European Commission
Justice, Fundamental Rights and Citizenship

Rue de la Loi, 200
B-1049 Brussels
T. +32 2 298 16 00

Brussels, 10 June 2013

Dear Attorney General,

I have serious concerns about recent media reports that United States authorities are accessing and processing, on a large scale, the data of European Union citizens using major US online service providers. Programmes such as PRISM and the laws on the basis of which such programmes are authorised could have grave adverse consequences for the fundamental rights of EU citizens.

The respect for fundamental rights and the rule of law are the foundations of the EU-US relationship. This common understanding has been, and must remain, the basis of cooperation between us in the area of Justice.

This is why, at the Ministerial of June 2012, you and I reiterated our joint commitment to providing citizens of the EU and of the US with a high level of privacy protection. On my request, we also discussed the need for judicial remedies to be available to EU citizens when their data is processed in the US for law enforcement purposes.

It is in this spirit that I raised with you already last June the issue of the scope of US legislation such as the Patriot Act. It can lead to European companies being required to transfer data to the US in breach of EU and national law. I argued that the EU and the US have already agreed formal channels of cooperation, notably a Mutual Legal Assistance Agreement, for the exchange of data for the prevention and investigation of criminal activities. I must underline that these formal channels should be used to the greatest possible extent, while direct access of US law enforcement authorities to the data of EU citizens on servers of US companies should be excluded unless in clearly defined, exceptional and judicially reviewable situations.

Mr Eric H. Holder, Jr.
Attorney General of the United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001
United States of America

Trust that the rule of law will be respected is also essential to the stability and growth of the digital economy, including transatlantic business. It is of paramount importance for individuals and companies alike. In this context, programmes such as PRISM can undermine the trust of EU citizens and companies in the Safe Harbour scheme which is currently under review in the EU legislative process.

Against this backdrop, I would request that you provide me with explanations and clarifications on the PRISM programme, other US programmes involving data collection and search, and laws under which such programmes may be authorised.

In particular:

1. *Are PRISM, similar programmes and laws under which such programmes may be authorised, aimed only at the data of citizens and residents of the United States, or also – or even primarily – at non-US nationals, including EU citizens?*

2. *(a) Is access to, collection of or other processing of data on the basis of the PRISM programme, other programmes involving data collection and search, and laws under which such programmes may be authorised, limited to specific and individual cases?*

   (b) If so, what are the criteria that are applied?

3. *On the basis of the PRISM programme, other programmes involving data collection and search, and laws under which such programmes may be authorised, is the data of individuals accessed, collected or processed in bulk (or on a very wide scale, without justification relating to specific individual cases), either regularly or occasionally?*

4. *(a) What is the scope of the PRISM programme, other programmes involving data collection and search, and laws under which such programmes may be authorised? Is the scope restricted to national security or foreign intelligence, or is the scope broader?*

   (b) How are concepts such as national security or foreign intelligence defined?

5. *What avenues, judicial or administrative, are available to companies in the US or the EU to challenge access to, collection of and processing of data under PRISM, similar programmes and laws under which such programmes may be authorised?*

6. *(a) What avenues, judicial or administrative, are available to EU citizens to be informed of whether they are affected by PRISM, similar programmes and laws under which such programmes may be authorised?*

   (b) How do these compare to the avenues available to US citizens and residents?

7. *(a) What avenues are available, judicial or administrative, to EU citizens or companies to challenge access to, collection of and processing of their personal data under PRISM, similar programmes and laws under which such programmes may be authorised?*

   (b) How do these compare to the avenues available to US citizens and residents?

Given the gravity of the situation and the serious concerns expressed in public opinion on this side of the Atlantic, you will understand that I will expect swift and concrete answers to these questions on Friday 14 June, when we meet at the EU-US Justice Ministerial. As you know, the European Commission is accountable before the European Parliament, which is likely to assess the overall trans-Atlantic relationship also in the light of your responses.

Yours sincerely,

[redacted]

ARES (2013) 2230328

VIVIANE REDING
VICE-PRESIDENT OF THE EUROPEAN COMMISSION
JUSTICE, FUNDAMENTAL RIGHTS AND CITIZENSHIP

CECILIA MALMSTRÖM
MEMBER OF THE EUROPEAN COMMISSION
HOME AFFAIRS

Brussels, 19 June 2013

Dear Attorney General,

On Friday 14 June 2013 in Dublin we had a first discussion of programmes which appear to enable United States authorities to access and process, on a large scale, the personal data of European individuals. We reiterated our concerns about the consequences of these programmes for the fundamental rights of Europeans, while you gave initial indications regarding the situation under U.S. law.

At our meeting, you were not yet in a position to answer all the questions set out in the letter of 10 June 2013. Given the strength of feeling and public opinion on this side of the Atlantic, we should be grateful if you would communicate your answers to those questions as soon as possible. We are particularly concerned about the volume of data collected, the personal and material scope of the programmes and the extent of judicial oversight and redress available to Europeans.

In addition, we welcome your proposal to set up a high-level group of EU and U.S. data protection and security experts to discuss these issues further. On the EU side it will be chaired by the European Commission and include Member States' experts both from the field of data protection and security, including law enforcement and intelligence/anti-terrorism.

We suggest that we convene the initial meeting of this group in July. Our intention is to ensure that the European Commission will be in a position to report, on the basis of the findings of the group, to the European Parliament and to the Council of the EU in October.

We look forward to your reply.

Yours sincerely,

[redacted]

[redacted]

Viviane Reding

Cecilia Malmström

Mr Eric H. Holder, Jr.
Attorney General of the United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001
United States of America

European Commission – rue de la Loi 200, B-1049 Brussels
eMail : Cecilia.Malmstrom@ec.europa.eu; Viviane.Reding@ec.europa.eu

ARES (2013) 2309328

VIVIANE REDING
VICE-PRESIDENT OF THE EUROPEAN COMMISSION
JUSTICE, FUNDAMENTAL RIGHTS AND CITIZENSHIP

CECILIA MALMSTRÖM
MEMBER OF THE EUROPEAN COMMISSION
HOME AFFAIRS

Brussels, 19 June 2013

Dear Secretary,

On Friday 14 June 2013 in Dublin we had a first discussion of programmes which appear to enable United States authorities to access and process, on a large scale, the personal data of European individuals. We reiterated our concerns about the consequences of these programmes for the fundamental rights of Europeans, while you gave initial indications regarding the situation under U.S. law.

At our meeting, you were not yet in a position to answer all the questions set out in the letter of 10 June 2013. Given the strength of feeling and public opinion on this side of the Atlantic, we should be grateful if you would communicate your answers to those questions as soon as possible. We are particularly concerned about the volume of data collected, the personal and material scope of the programmes and the extent of judicial oversight and redress available to Europeans.

In addition, we welcome your proposal to set up a high-level group of EU and U.S. data protection and security experts to discuss these issues further. On the EU side it will be chaired by the European Commission and include Member States' experts both from the field of data protection and security, including law enforcement and intelligence/anti-terrorism.

We suggest that we convene the initial meeting of this group in July. Our intention is to ensure that the European Commission will be in a position to report, on the basis of the findings of the group, to the European Parliament and to the Council of the EU in October.

We look forward to your reply.

Yours sincerely,

[redacted]

Viviane Reding

[redacted]

Cecilia Malmström

Secretary Janet Napolitano
Department of Homeland Security
U.S. Department of Homeland Security
Washington, D.C. 20528
United States of America

European Commission – rue de la Loi 200, B-1049 Brussels
eMail : Cecilia.Malmstrom@ec.europa.eu; Viviane.Reding@ec.europa.eu

Date de réception : 23/01/2015

Published ID	:	C-362/14
Document number	:	13
Register number	:	976996
Date of lodgment	:	03/11/2014
Date of entry in the register	:	03/11/2014
Type of document	:	Observations
	:	Annexes Part 2
Lodgment reference	:	DC33346
File number	:	3
Person lodging document	:	Julie Vondung (R249125) Commission

Annex 2

Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU", COM(2013) 847, 27.11.2013, referred to in paragraph 29 of the observations.

EUROPEAN
COMMISSION

Brussels, 27.11.2013
COM(2013) 847 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU

1. INTRODUCTION

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "data protection Directive") sets the rules for transfers of personal data from EU Member States to other countries outside the EU[1] to the extent such transfers fall within the scope of this instrument[2].

Under the Directive, the Commission may find that a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into in order to protect rights of individuals in which case the specific limitations on data transfers to such a country would not apply. These decisions are commonly referred to as "**adequacy decisions**".

On 26 July 2000, the Commission adopted Decision 520/2000/EC[3] (hereafter "**Safe Harbour decision**") recognising the Safe Harbour Privacy Principles and Frequently Asked Questions (respectively "the Principles" and "FAQs"), issued by the Department of Commerce of the United States, as providing adequate protection for the purposes of personal data transfers from the EU. The Safe Harbour decision was taken following an opinion of the Article 29 Working Party and an opinion of the Article 31 Committee delivered by a qualified majority of Member States. In accordance with Council Decision 1999/468 the Safe Harbour Decision was subject to prior scrutiny by the European Parliament.

As a result, the current Safe Harbour decision allows free transfer[4] of personal information from EU Member States[5] to companies in the US which have signed up to the Principles in circumstances where the transfer would otherwise not meet the EU standards for adequate level of data protection given the substantial differences in privacy regimes between the two sides of Atlantic.

The functioning of the current Safe Harbour arrangement relies on commitments and self-certification of adhering companies. Signing up to these arrangements is voluntary, but the rules are binding for those who sign up. The fundamental principles of such an arrangement are:

a) Transparency of adhering companies' privacy policies,

b) Incorporation of the Safe Harbour principles in companies' privacy policies, and

---

1 Articles 25 and 26 of the data protection Directive set forth the legal framework for transfers of personal data from the EU to third countries outside the EEA.

2 Additional rules have been laid down in Article 13 of Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters to the extent such transfers concern personal data transmitted or made available by one Member State to another Member State, who subsequently intends to transfer those data to a third state or international body for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions.

3 Commission decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce in OJ 215 of 28 August 2000, page 7.

4 The above does not exclude the application to the data processing of other requirements that may exist under national legislation implementing the EU data protection directive.

5 Data transfers from the three States Parties to the EEA are similarly affected, following extension of Directive 95/46/EC to the EEA Agreement, Decision 38/1999 of 25 June 1999, OJ L 296/41, 23.11.2000.

c) Enforcement, including by public authorities.

This fundamental basis of the Safe Harbour has to be reviewed in the **new context** of:

a) the exponential increase in data flows which used to be ancillary but are now central to the rapid growth of the digital economy and the very significant developments in data collection, processing and use,

b) the critical importance of data flows notably for the transatlantic economy,[6]

c) the rapid growth of the number of companies in the US adhering to the Safe Harbour scheme which has increased by eight-fold since 2004 (from 400 in 2004 to 3,246 in 2013),

d) the information recently released on US surveillance programmes which raises new questions on the level of the protection the Safe Harbour arrangement is deemed to guarantee.

Against this background, this Communication takes stock of the functioning of the Safe Harbour scheme. It is **based on evidence** gathered by the Commission, the work of the EU-US Privacy Contact Group in 2009, a Study prepared by an independent contractor in 2008[7] and information received in the ad hoc EU-U.S Working Group (the "Working Group") established following the revelations on US surveillance programmes *(see a parallel Document)*. This Communication follows the two **Commission Assessment Reports** in the start-up period of the Safe Harbour arrangement, respectively in 2002[8] and 2004[9].

2. STRUCTURE AND FUNCTIONING OF SAFE HARBOUR

2.1. Structure of the Safe Harbour

A US company that wants to adhere to the Safe Harbour must: (a) identify in its publicly available privacy policy that it adheres to the Principles and actually does comply with the Principles, as well as (b) self-certify i.e., declare to the US Department of Commerce that it is in compliance with the Principles. The self-certification must be resubmitted on an annual basis. The Safe Harbour Privacy Principles attached in Annex I to the Safe Harbour Decision include requirements on both the substantive protection of personal data (data integrity, security, choice, and onward transfer principles) and the procedural rights of data subjects (notice, access, and enforcement principles).

As to the enforcement of the Safe Harbour scheme in the US, two US institutions play a major role: the US Department of Commerce and the US Federal Trade Commission.

The **Department of Commerce** reviews every Safe Harbour self-certification and every annual recertification submission that it receives from companies to ensure that they include

---

6 According to some studies, if services and cross-border data flows were to be disrupted as a consequence of discontinuity of binding corporate rules, model contract clauses and the Safe Harbour, the negative impact on EU GDP could reach -0,8% to -1,3% and EU services exports to the US would drop by -6,7% due to loss of competitiveness. See: "The Economic Importance of Getting Data Protection Right", a study by the European Centre for International Political Economy for the US Chamber of Commerce, March 2013.

7 Impact Assessment Study prepared for the European Commission in 2008 by the *Centre de Recherche Informatique et Droit* ('CRID') of the University of Namur.

8 Commission Staff Working Paper "The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce", SEC (2002) 196, 13.12.2002.

9 Commission Staff Working Paper "The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce", SEC (2004) 1323, 20.10.2004.

all the elements required to be a member of the scheme[10]. It updates a list of companies which have filed self-certification letters and publishes the list and letters on its website. Furthermore, it monitors the functioning of Safe Harbour and removes from the list companies not complying with the Principles.

The **Federal Trade Commission**, within its powers in the field of consumer protection, intervenes against unfair or deceptive practices pursuant to Section 5 of the Free Trade Commission Act. The Federal Trade Commission's enforcement actions include inquiries on false statements of adherence to Safe Harbour and non-compliance with these Principles by companies which are members of the scheme. In the specific cases of enforcing the Safe Harbour Principles against air carriers, the competent body is the US Department of Transportation[11].

The current Safe Harbour Decision is part of EU law which has to be applied by Member State Authorities. Under the Decision, the EU national **data protection authorities** (DPAs) have the right to suspend data transfers to Safe Harbour certified companies in specific cases[12]. The Commission is not aware of any cases of suspension by a national data protection authority since the establishment of Safe Harbour in 2000. Independently of the powers they enjoy under the Safe Harbour Decision, EU national data protection authorities are competent to intervene, including in the case of international transfers, in order to ensure compliance with the general principles of data protection set forth in the 1995 Data Protection Directive.

As recalled in the current Safe Harbour Decision, it is **the competence of the Commission** – acting in accordance with the examination procedure set out in Regulation 182/2011 – to adapt the Decision, to suspend it or limit its scope at any time, in the light of experience with its implementation. This is notably foreseen if there is a systemic failure on the US side, for example if a body responsible for ensuring compliance with the Safe Harbour Privacy Principles in the United States is not effectively fulfilling its role, or if the level of protection provided by the Safe Harbour Principles is overtaken by the requirements of US legislation. As with any other Commission decision, it can also be amended for other reasons or even revoked.

2.2. The functioning of the Safe Harbour

The **3246**[13] **certified companies** include both small and big companies[14]. While financial services and telecommunication industries are outside the Federal Trade Commission enforcement powers and therefore excluded from the Safe Harbour, many industry and services sectors are present among certified companies, including well known Internet companies and industries ranging from information and computer services to pharmaceuticals, travel and tourism services, healthcare or credit card services[15]. These are mainly US companies that provide services in the EU internal market. There are also subsidiaries of some

---

10 If a company's certification or recertification fails to meet Safe Harbour requirements, the Department of Commerce notifies the company requesting steps to be taken (e.g., clarifications, changes in policy description) before the company's certification may be finalised.

11 Under Title 49 of the US Code Section 41712.

12 More specifically, suspension of transfers can be required in two situations, where:
(a) the government body in the US has determined that the company is violating the Safe Harbour Privacy Principles; or
(b) there is a substantial likelihood that the Safe Harbour Privacy Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the company with notice and an opportunity to respond.

13 On 26 September 2013 the number of Safe Harbour organizations listed as "**current**" on the Safe Harbour List was **3246**, as "**not current**" **935.**

14 Safe Harbour organizations with 250 or less employees: 60% (1925 of 3246). Safe Harbour organizations with 251 or more employees: **40%** (1295 of 3246).

15 For example MasterCard deals with thousands of banks and the company is a clear example of a case where Safe Harbour cannot be replaced by other legal instruments for personal data transfers such as binding corporate rules or contractual arrangements.

EU firms such as Nokia or Bayer. 51% are firms that process data of employees in Europe transferred to the US for human resource purposes[16].

There has been a **growing concern** among some data protection authorities in the EU about data transfers under the current Safe Harbour scheme. Some Member States' data protection authorities have criticised the very general formulation of the principles and the high reliance on self-certification and self-regulation. Similar concerns have been raised by industry, referring to distortions of competition due to a lack of enforcement.

The current Safe Harbour arrangement is based on the voluntary adherence of companies, on self-certification by these adhering companies and on enforcement of the self-certification commitments by public authorities. In this context any lack of transparency and any shortcomings in enforcement undermine the foundations on which the Safe Harbour scheme is constructed.

Any gap in transparency or in enforcement on the US side results in responsibility being shifted to European data protection authorities and to the companies which use the scheme. On 29 April 2010 German data protection authorities issued a decision requesting companies transferring data from Europe to the US to actively check that companies in the US importing data actually comply with Safe Harbour Privacy Principles and recommending that "at least the exporting company must determine whether the Safe Harbour certification by the importer is still valid"[17].

On 24 July 2013, following the revelations on US surveillance programmes, German DPAs went a step further expressing concerns that "there is a substantial likelihood that the principles in the Commission's decisions are being violated"[18]. There are cases of some DPAs (e.g., Bremen DPA) that have requested a company transferring personal data to US providers to inform the DPA on whether and how the concerned providers prevent access by the National Security Agency. The Irish DPA has reported that it received two complaints recently which reference the Safe Harbour programme following coverage about the US Intelligence Agencies programmes but declined to investigate them on the basis that the transfer of personal data to a third country met the requirements of Irish data protection law. Following a similar complaint, the Luxembourg DPA has found that Microsoft and Skype have complied with the Luxembourg Data Protection Act when transferring data to US[19]. However, the Irish High Court has since granted an application for judicial review under which it will review the inaction of the Irish Data Protection Commissioner in relation to the US surveillance programmes. One of the two complaints was filed by a student group Europe v Facebook (EvF) which also filed similar complaint against Yahoo in Germany, which is being processed by the relevant data protection authorities.

These divergent responses of data protection authorities to the surveillance revelations demonstrate the real risk of the fragmentation of the Safe Harbour scheme and raise questions as to the extent to which it is enforced.

---

16 Safe Harbour organizations that cover organization human resources data under their Safe Harbour certification (and thereby have agreed to cooperate and comply with the EU data protection authorities): **51%** (1671 of 3246).

17 See Düsseldorfer Kreis decision of 28/29 April 2010 . See: Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile However, the European Data Protection Supervisor (EDPS) Peter Hustinx expressed an opinion at the European Parliament LIEBE Committee Inquiry on 7 October 2013 that "substantial improvements have been made and most issues now been settled" as far as Safe Harbour is concerned: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf

18 See a resolution of a German Conference of data protection commissioners underlying that intelligence services constitute a massive threat to data traffic between Germany and countries outside Europe: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

19 See the press statement of Luxemboug DPA on 18 November 2013.

3. TRANSPARENCY OF ADHERED COMPANIES' PRIVACY POLICIES

Under the FAQ 6 that is annexed to the Safe Harbour Decision (Annex II) companies interested in certifying under the Safe Harbour must provide to the Department of Commerce and make public their privacy policy. It must include a commitment to adhere to the Privacy Principles. The requirement to **make publicly available the privacy policies** of self-certified companies as well as their statement to adhere to the Privacy Principles is critical for the operation of the scheme.

Insufficient accessibility to privacy policies of such companies is to the detriment of individuals whose personal data is being collected and processed, and may constitute a **violation of the principle of notice**. In such cases, individuals whose data is being transferred from the EU may be unaware of their rights and the obligations to which a self-certified company is subjected.

Moreover, the commitment by companies to comply with the Privacy Principles **triggers the Federal Trade Commission's powers to enforce these principles** against companies in cases of non-compliance as an unfair or deceptive practice. Lack of transparency by companies in the US renders Federal Trade Commission oversight more difficult and undermines the effectiveness of enforcement.

Over the years a substantial number of self-certified companies had not made their privacy policy public and/or had not made a public statement of adherence to the Privacy Principles. The 2004 Safe Harbour report pointed to the necessity for the Department of Commerce to **adopt a more active stance in scrutinising compliance** with this requirement.

Since 2004, the Department of Commerce has developed **new information tools** aimed at helping companies to comply with their transparency obligations. The relevant information on the scheme is accessible on the Department of Commerce's website dedicated to the Safe Harbour[20] that also allows companies to upload their privacy policies. The Department of Commerce has reported that companies have made use of this feature and posted their privacy policies on the Department of Commerce website when applying to join the Safe Harbour[21]. In addition, the Department of Commerce published in 2009-2013 a series of guidelines for companies wishing to join Safe Harbour, such as a "Guide to Self-Certification" and "Helpful Hints on Self-Certifying Compliance"[22].

The degree of compliance with the transparency obligations varies amongst companies. Whereas certain companies limit themselves to notifying to the Department of Commerce a description of their privacy policy as part of the self-certification process, the majority make these policies public on their websites, in addition to uploading them on the Department of Commerce website. However, these **policies are not always presented in a consumer-friendly and easily readable form**. Hyperlinks to privacy policies do not always function properly nor do they always refer to the correct webpages.

It follows from the Decision and its annexes that the requirement that companies should publicly disclose their privacy policies **goes beyond mere notification** of self-certification to the Department of Commerce. The requirements for certification as set out in the FAQs include a description of the privacy policy and transparent information on where it is available for viewing by the public[23]. Privacy policy statements must be clear and easily accessible by

---

20 http://www.export.gov/SafeHarbour/

21 https://SafeHarbour.export.gov/list.aspx

22 The Guide is available on the programme's website at: http://export.gov/SafeHarbour/ Helpful Hints: http://export.gov/SafeHarbour/eu/eg_main_018495.asp

23 On 12 November 2013 the Department of Commerce has confirmed that "Today, companies that have public websites and cover consumer/client/visitor data must include a Safe Harbor-compliant privacy policy on their respective websites" (document: "U.S.-EU Cooperation to Implement the Safe Harbor Framework" of 12 Nov. 2013).

the public. They must include a hyperlink to the Department of Commerce Safe Harbour website which lists all the 'current' members of the scheme and a link to the alternative dispute resolution provider. However, a number of companies under the scheme in the period 2000-2013 failed to comply with these requirements. During working contacts with the Commission in February 2013 the Department of Commerce has acknowledged that up to 10% of certified companies may actually not have posted a privacy policy containing the Safe Harbour affirmative statement on their respective public websites.

Recent statistics demonstrate also a persisting problem of **false claims of Safe Harbour adherence**. About 10% of companies claiming membership in the Safe Harbour are not listed by the Department of Commerce as current members of the scheme[24]. Such false claims originate from both: companies which have never been participants of the Safe Harbour and companies which have once joined the scheme but then failed to resubmit their self-certification to the Department of Commerce at the yearly intervals. In this case they continue to be listed on the Safe Harbour website, but with certification status "not current", meaning that the company has been a member of the scheme and thus has an obligation to continue to provide protection to data already processed. The Federal Trade Commission is competent to intervene in cases of deceptive practices and non-compliance of the Safe Harbour principles (see Section 5.1). Unclarity over the "false claims" impacts the credibility of the scheme.

The European Commission alerted the Department of Commerce through regular contacts in 2012 and 2013 that, in order to comply with the transparency obligations, it is not sufficient for companies to only provide the Department of Commerce with a description of their privacy policy. Privacy policy statements must be made publicly available. The Department of Commerce was also asked to **intensify its periodic controls of companies' websites** subsequent to the verification procedure carried out in the context of the first self-certification process or its annual renewal and to take action against those companies which do not comply with the transparency requirements.

As a first answer to EU concerns, **the Department of Commerce has since March 2013 made it mandatory** for a Safe Harbour company with a public website to make its privacy policy for customer/user data readily available on its public website. At the same time, the Department of Commerce began notifying all companies whose privacy policy did not already include a link to Department of Commerce Safe Harbour website that one should be added, making the official Safe Harbour List and website directly accessible to consumers visiting a company's website. This will allow European data subjects to verify immediately, without additional searches in the web, a company's commitments submitted to the Department of Commerce. Additionally, the Department of Commerce started notifying companies that contact information for their independent dispute resolution provider should be included in their posted privacy policy[25].

This process needs to be speeded up to ensure that all certified companies fully meet Safe Harbour requirements not later than by March 2014 (i.e. by companies' yearly recertification deadline, counting from the introduction of new requirements in March 2013).

---

[24] In September 2013 an Australian consultancy Galexia compared Safe Harbour membership "false claims" in 2008 and 2013. Its main finding is that, in parallel to the increase of membership in the Safe Harbour between 2008 and 2013 (from 1,109 to 3,246), the number of false claims has increased from 206 to 427. http://www.galexia.com/public/about/news/about_news-id225.html

[25] Between March and September 2013 the Department of Commerce has:
- Notified the 101 companies *who had already uploaded their Safe Harbour compliant privacy policy to Safe Harbour website* that they must also post their privacy policy to their company websites;
- Notified the 154 companies that had not already done so, that they should include a link to Safe Harbour website in their privacy policy;
- Notified more than 600 companies that they should include contact information for their independent dispute resolution provider in their privacy policy.

Nevertheless, concerns remain as to whether all self-certified companies fully comply with the transparency requirements. Compliance with the obligations undertaken at the point of the initial self-certification and the annual renewal should be monitored and investigated more stringently by the Department of Commerce.

4. INTEGRATION OF THE SAFE HARBOUR PRIVACY PRINCIPLES IN COMPANIES' PRIVACY POLICIES

Self-certified companies must comply with the Privacy Principles set out in Annex I to the Decision in order to obtain and retain the benefit of the Safe Harbour.

In the 2004 report, the Commission found that a significant number of **companies had not correctly incorporated the Safe Harbour Privacy Principles** in their data processing policies. For example, individuals were not always given clear and transparent information about the purposes for which their data were processed or were not given the possibility to opt out if their data were to be disclosed to a third party or to be used for a purpose that was incompatible with the purposes for which it was originally collected. The 2004 Commission's report considered that the Department of Commerce *" should be more proactive with regard to access to the Safe Harbour and to awareness of the Principles "*[26].

There has been limited progress in that respect. Since 1 January 2009, any company seeking to renew its certification status for Safe Harbour – which must be renewed annually – has had its privacy policy evaluated by the Department of Commerce prior to the renewal. The evaluation is however limited in scope. There is **no full evaluation of the actual practice** in the self-certified companies which would significantly increase the credibility of the self-certification process.

Further to the Commission's requests for a more rigorous and systematic oversight of the self-certified companies by the Department of Commerce, **more attention is currently applied to new submissions**. The number of new submissions which have not been accepted, but are resent to companies for improvements in privacy policies has significantly increased between 2010 and 2013: doubled for re-certifying companies and tripled for the Safe Harbour newcomers[27]. The Department of Commerce has assured the Commission that any certification or recertification can be finalised only if the company's privacy policy fulfils all requirements, notably that it includes an affirmative commitment to adhere to the relevant set of Safe Harbour Privacy Principles and that the privacy policy is publicly available. A company is required to identify in its Safe Harbour List record the location of the relevant policy. It is also required to clearly identify on its website an Alternative Dispute Resolution provider and include a link to the Safe Harbour self-certification on the website of the Department of Commerce. However, it has been estimated that over 30% of Safe Harbour members do not provide dispute resolution information in the privacy policies on their websites[28].

A majority of the companies that the Department of Commerce has removed from the Safe Harbour List were removed at the express request of the relevant companies (e.g., companies that had merged or were acquired, had changed their lines of business or had gone out of business). A smaller number of records of lapsed companies have been removed when the

---

[26] See page 8 of the 2004 Report SEC (2004) 1323.

[27] According to statistics provided in September 2013 by the Department in Commerce, the DoC notified in 2010 18% (93) of the 512 first-time certifiers and 16% (231) of the 1,417 recertifiers to make improvements to their privacy policies and/or Safe Harbour applications. However, as a follow up to Commission requests for severe, diligent and systematic scrutiny of all submissions, through mid-Sep. 2013, DoC notified 56% (340) of the 602 first-time certifiers and 27% (493) of the 1,809 recertifiers asking them to make improvements to their privacy policies.

[28] Chris Connolly (Galexia) appearance before the European Parliament LIBE Committee inquiry on 7 Oct. 2013.

websites that were listed in the records appeared to be inoperative and the companies' certification status had been "Not current" for several years[29]. Importantly, none of these removals seems to have taken place because the Department of Commerce verification led to the identification of compliance problems.

The Safe Harbour List record serves as a public notice and as a record of a company's Safe Harbour commitments. **The commitment to adhere to the Safe Harbour Principles is not time-limited** with respect to data received during the period in which the company enjoys the benefit of the Safe Harbour, and the company must continue to apply the Principles to such data as long as it stores, uses or discloses them, even if it leaves the Safe Harbour for any reason.

The number of Safe Harbour **applicants that did not pass administrative review** by the Department of Commerce and therefore were never added to the Safe Harbour List is the following: **In 2010**, only **6%** (33) of the 513 first-time certifiers were never included in the Safe Harbour List because they did not comply with Department of Commerce standards for self-certification. In **2013, 12%** (75) of the 605 first-time certifiers were never included in the Safe Harbour List because they have not complied with Department of Commerce standards for self-certification.

As a minimum requirement to increase the transparency of the oversight, the Department of Commerce should list on its website all companies that have been removed from the Safe Harbour and indicate reasons for which the certification has not been renewed. The label "Not current" on the Department of Commerce list of Safe Harbour member companies should be regarded not just as information but should be accompanied by **a clear warning** – both verbal and graphical - that a company is currently not fulfilling Safe Harbour requirements.

Moreover, some companies still fall short of fully incorporating all Safe Harbour Principles. Apart from the issue of transparency addressed in Section 3 above, privacy policies of self-certified companies are often unclear as regards the purposes for which data is collected, and the right to choose whether or not data can be disclosed to third parties; thereby raising issues of compliance with the Privacy Principles of "Notice" and "Choice". Notice and choice are crucial to ensure control from data subjects over what happens to their personal information.

The critical first step in the compliance process, the incorporation of the Safe Harbour Privacy Principles in companies' privacy policies, is not sufficiently ensured. The Department of Commerce should address it as a matter of priority by developing a methodology of compliance in the operational practice of companies and their interaction with clients. **There must be an active follow up by the Department of Commerce on effective incorporation of the Safe Harbour principles in companies' privacy policies**, rather than leaving enforcement action only to be triggered by complaints of individuals.

5. ENFORCEMENT BY PUBLIC AUTHORITIES

A number of mechanisms are available to ensure effective enforcement of the Safe Harbour scheme and to offer recourse for individuals in cases where the protection of their personal information is affected by non-compliance with the Privacy Principles.

According to the "Enforcement" Principle, privacy policies of self-certified organizations must include effective compliance mechanisms. Pursuant to the "Enforcement" Privacy Principle as further clarified by FAQ 11, FAQ 5 and FAQ 6, this requirement can be met by

[29] As of December 2011, the US Department of Commerce had removed 323 companies from the Safe Harbour List: 94 companies were removed because they were no longer in business; 88 companies due to acquisition or merger, 95 at the requests of the parent company; 41 companies because repeated failure to ask for recertification and 5 companies for miscellaneous reasons.

adhering to **independent recourse mechanisms** that have publicly stated their competence to hear individual complaints for failure to abide by the Principles. Alternatively, this can be achieved through the organization's commitment to cooperate with the **EU Data Protection Panel**[30]. Moreover self-certified companies are subject to the jurisdiction of the Federal Trade Commission under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce[31].

The 2004 Report expressed concerns as regards the enforcement of the Safe Harbour scheme, namely that the Federal Trade Commission should be more proactive in launching investigations and raising awareness of individuals about their rights. Another area of concern was the lack of clarity in relation to the Federal Trade Commission's competence to enforce the Principles regarding human resources data.

The recourse body responsible for human resources data – the EU Data Protection Panel – has received one complaint concerning human resources data[32]. However, the absence of complaints does not allow conclusions to be drawn as to the full functioning of the scheme. Ex-officio checks of companies' compliance should be introduced to verify the actual implementation of data protection commitments. EU Data Protection Authorities should also undertake actions in order to raise awareness of the existence of the Panel.

Problems have been highlighted in relation to the way in which alternative recourse mechanisms function as enforcement bodies. A number of these bodies lack appropriate means to remedy cases of failure to comply with the Principles. This shortcoming needs to be addressed.

5.1. Federal Trade Commission

The Federal Trade Commission can take enforcement measures in case of violations of the Safe Harbour commitments that companies make. When Safe Harbour was established, the Federal Trade Commission committed to review on a priority basis all referrals from EU Member State authorities[33]. Since no complaints were received for the first ten years of the arrangement, the Federal Trade Commission decided to seek to identify any Safe Harbour violations in every privacy and data security investigation it conducts. Since 2009, the Federal Trade Commission has brought 10 enforcement actions against companies based on Safe Harbour violations. These actions notably resulted in settlement orders – subject to substantial penalties – prohibiting privacy misrepresentations, including of compliance with the Safe Harbour, and imposing on companies' comprehensive privacy programmes and audits for 20 years. The companies must accept independent assessments of their privacy programmes on the request of the Federal Trade Commission. These assessments are reported regularly to the Federal Trade Commission. The Federal Trade Commission's orders also prohibit these companies from misrepresenting their privacy practices and their participation in Safe Harbour or similar privacy schemes. This was the case for example in the Federal Trade

---

30 The EU Data Protection Panel is a body competent for investigating and resolving complaints lodged by individuals for alleged infringement of the Safe Harbour Principles by an US company member of the Safe Harbour. Companies that certify to the Safe Harbour Principles must choose to comply with independent recourse mechanism or to cooperate with the EU Data Protection Panel in order to remedy problems arising out of failure to comply with Safe Harbour Principles. Cooperation with the EU Data Protection Panel is nonetheless mandatory when the US company processes human resources personal data transferred from the EU in the context of an employment relationship. If the company commits itself to cooperate with the EU panel, it must also commit itself to comply with any advice given by the EU panel where it takes the view that the company needs to take specific action to comply with the Safe Harbour Principles, including remedial or compensatory measures.

31 The Department of Transportation exercises similar jurisdictions over air carriers under Title 49 United States Code Section 41712.

32 The complaint originated from a Swiss citizen and therefore has been referred by the EU Data Protection Panel to the Swiss data protection authority (US has a separate Safe Harbour scheme for Switzerland).

33 See Annex V to the Commission Decision 2000/520/EC of 26 July 2000.

Commission investigations against Google, Facebook and Myspace.[34] In 2012 Google agreed to pay a $22.5 million fine to settle allegations that it violated a consent order. In all privacy investigations the Federal Trade Commission ex officio examines whether there is Safe Harbour violation.

The Federal Trade Commission has reiterated recently its declarations and commitment to reviewing, on a priority basis, any referrals received from privacy self-regulatory companies and EU Member States that allege a company's non-compliance with Safe Harbour Principles.[35] The Federal Trade Commission has received only a few referrals from European data protection authorities over the past three years.

Transatlantic cooperation between data protection authorities started to develop in recent months. For example the Federal Trade Commission signed on 26 June 2013 with the Office of the Data Protection Commissioner of Ireland a Memorandum of Understanding on mutual assistance in the enforcement of laws protecting personal information in the private sector. The memorandum establishes a framework for increased, more streamlined, and more effective privacy enforcement cooperation[36].

In August 2013, the Federal Trade Commission announced a further reinforcement of the checks on companies with control over large databases of personal information. It has also created a portal where consumers can file a privacy complaint regarding a US company[37].

The Federal Trade Commission should also increase efforts to investigate false claims of Safe Harbour adherence. A company claiming on its website that it complies with the Safe Harbour requirements, but is not listed by the Department of Commerce as a 'current' member of the scheme, is misleading consumers and abusing their trust. False claims weaken the credibility of the system as a whole and therefore should be immediately removed from the companies' websites. The companies should be bound by an enforceable requirement not to mislead consumers. The Federal Trade Commission should continue seeking to identify Safe Harbour false claims as the one in the *Karnani* case, where the Federal Trade Commission shut down a California website for claiming a false Safe Harbour registration, and engaging in fraudulent e-commerce practices targeted at European consumers[38].

On 29 October 2013 the Federal Trade Commission announced that it had opened "numerous investigations into Safe Harbor compliance in recent months" and that more enforcement actions on this front can be expected "in the coming months". The Federal Trade Commission confirmed also that it is "committed to looking for ways to improve its efficacy" and would "continue to welcome any substantive leads, such as the complaint received in the past month from a European-based consumer advocate alleging a large number of Safe Harbor-related violations".[39] The agency committed also to "systematically monitor compliance with Safe Harbor orders, as we do with all our orders"[40].

---

34 Over the period 2009-2012 Federal Trade Commission has completed ten enforcement actions of Safe Harbour commitments: FTC v. Javian Karnani, and Balls of Kryptonite, LLC (2009), World Innovators, Inc. (2009), Expat Edge Partners, LLC (2009), Onyx Graphics, Inc. (2009), Directors Desk LLC (2009), Progressive Gaitways LLC (2009), Collectify LLC (2009), Google Inc. (2011), Facebook, Inc. (2011), Myspace LLC (2012). See: "Federal Trade Commission of Safe Harbour Commitments": http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf See also: "Case Highlights": http://business.ftc.gov/us-eu-Safe-Harbour-framework. Most of these cases involved problems with companies that joined Safe Harbour but then continued to represent themselves as members without renewing the annual certification.

35 This commitment has been reiterated at a meeting of Federal Trade Commission Commissioner Julie Brill with EU Data protection Authorities (Article 29 Working Party) in Brussels on 17 April 2013.

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n

37 Consumers can file their complaints via the Federal Trade Commission Complaint Assistant (https://www.ftccomplaintassistant.gov/) and international consumers may file complaints via econsumer.gov (http://www.econsumer.gov).

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf and http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf

40 Letter of the Federal Trade Commission Chairwoman Edith Ramirez to Vice-President Viviane Reding.

On 12 November 2013, the Federal Trade Commission informed the European Commission that "**if a company's privacy policy promises Safe Harbor protections, that company's failure to make or maintain a registration, is not, by itself, likely to excuse that company from FTC enforcement of those Safe Harbor commitments**"[41].

In November 2013, the Department of Commerce informed the European Commission that "to help ensure that companies do not make 'false claims' of participation in Safe Harbor, the Department of Commerce will begin a process of contacting Safe Harbor participants one month prior to their recertification date to describe the steps they must follow should they chose not to recertify". **The Department of Commerce "will warn companies** in this category to remove all references to Safe Harbor participation, including use of Commerce's Safe Harbor certification mark, from the companies' privacy policies and websites, **and notify them clearly that failure to do so could subject the companies to FTC enforcement actions**"[42].

To combat false claims of Safe Harbour adherence, privacy policies of self-certified companies' websites should always include a link to the Department of Commerce Safe Harbour website where all the 'current' members of the scheme are listed. This will allow European data subjects to verify immediately, without additional searches whether a company is currently a member of the Safe Harbour. The Department of Commerce has started in March 2013 to request this from companies, but the process should be intensified.

The continuous monitoring and consequent enforcement by the Federal Trade Commission of actual compliance with the Safe Harbour Principles – in addition to the measures taken by the Department of Commerce as highlighted above – remains a key priority for ensuring proper and effective functioning of the scheme. It is necessary in particular to increase **ex-officio checks and investigations of companies' compliance** to the Safe Harbour principles. Complaints to the Federal Trade Commission relating violations should also be further facilitated.

5.2. EU Data Protection Panel

The EU Data Protection Panel is a body created under the Safe Harbour Decision. It is competent to investigate complaints lodged by individuals referring to personal data collected in the context of the employment relationship as well as cases relating to certified companies which have chosen this option for dispute resolution under the Safe Harbour (53% of all companies). It is composed of representatives of various EU data protection authorities.

To date, the Panel received four complaints (two in 2010 and two in 2013). It referred two complaints in 2010 to national data protection authorities (UK and Switzerland). The third and the fourth complaints are currently under examination. The low level of complaints can be explained by the fact that the powers of Panel are, as mentioned above, primarily limited to certain type of data.

The Panel's limited caseload could be also partly explained by the lack of awareness about the existence of the Panel. The Commission has, since 2004, made the information about the Panel more visible on its website[43].

---

41 Letter of the Federal Trade Commission Chairwoman Edith Ramirez to Vice-President Viviane Reding.

42 "U.S.-EU Cooperation to Implement the Safe Harbor Framework", 12 November 2013.

43 Pursuant to the 2004 report, an Information Notice in the form of Q&A of the EU Data Protection Panel has been published on the Commission's website (DG Justice) with the purpose of raising awareness of individuals and help them to file a complaint when they believe that their personal data has been processed in violation of the Safe Harbour: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf
The standard complaint form is available at http://ec.europa.eu/justice/policies/privacy/docs/adequacy/ complaint_form_en.pdf

To make a better use of the Panel, companies in the US which have chosen to cooperate with it and comply with its decisions, for some or all categories of personal data covered in their respective self-certifications, should clearly and prominently indicate it in their privacy policies commitments to allow the Department of Commerce to scrutinise this aspect. A dedicated page should be created on each EU data protection authority's website regarding Safe Harbour to raise Safe Harbour awareness with European companies and data subjects.

5.3. Improvement of enforcement

The weaknesses in transparency and weaknesses in enforcement that have been identified above, lead to concerns among European companies as regards the negative impact of the Safe Harbour scheme on European companies' competitiveness. Where a European company competes with a US company operating under Safe Harbour, but in practice not applying its principles, the European company is at a competitive disadvantage in relation to that US company.

Furthermore, the Federal Trade Commission's jurisdiction extends to unfair or deceptive acts or practices "in or affecting commerce". Section 5 of the Federal Trade Commission Act established exceptions to the Federal Trade Commission's authority over unfair or deceptive acts or practices with respect inter alia to **telecommunications.** Being outside Federal Trade Commission enforcement, telecom companies are not allowed to adhere to the Safe Harbour. However, with the growing convergence of technologies and services, many of their direct competitors in the US ICT sector are members of Safe Harbour. The exclusion of telecom companies from the data exchanges under the Safe Harbour scheme is a matter of concern to some European telecom operators. According to the European Telecommunications Network Operators' Association (ETNO) "this is in clear conflict to the most important plea of telecommunication operators regarding the need for a level playing field"[44].

6. STRENGTHENING THE SAFE HARBOUR PRIVACY PRINCIPLES

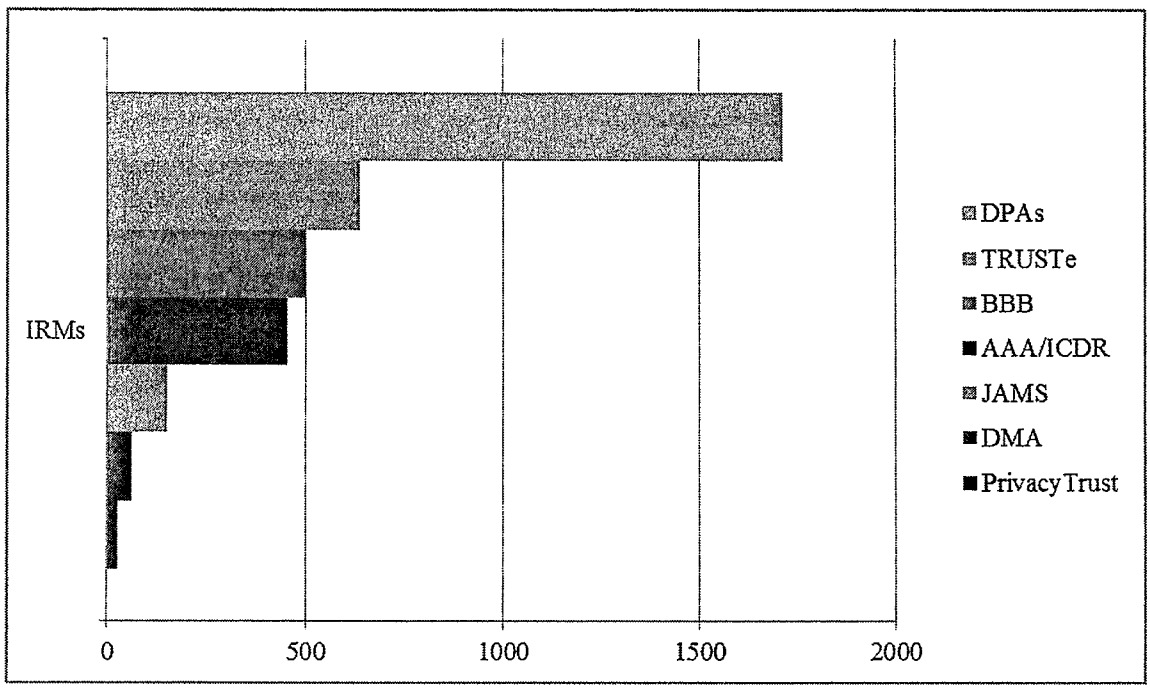
6.1. Alternative Dispute Resolutions

The enforcement principle requires that there must be "**readily available and affordable recourse mechanisms** by which each individual's complaints and disputes are investigated". To that end the Safe Harbour scheme establishes a system of Alternative Dispute Resolution (ADR) by an independent third party[45] to provide individuals with rapid solutions. The three top recourse mechanisms bodies are the EU Data Protection Panel, BBB (Better Business Bureaus) and TRUSTe.

---

44 "ETNO considerations" received by Commission services on 4 October 2013 discuss also 1) definition of personal data in Safe Harbour, 2) lack of monitoring of the Safe Harbour, 3) and the fact that "US companies can transfer data with much less restrictions than their European counterparts" which "constitutes a clear discrimination of European companies and is affecting the competitiveness of European companies". Under the Safe Harbour rules, to disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles.

45 The EU Directive 2013/11/EU on consumer ADR underlines the importance of independent, impartial, transparent, effective, fast and fair alternative dispute resolution procedures.



The use of ADR has increased since 2004 and the Department of Commerce has strengthened the monitoring of American ADR providers to make sure that the information they offer about the complaint procedure is clear, accessible and understandable. However, the effectiveness of this system is yet to be proven due to the limited number of cases dealt with so far[46].

Though the Department of Commerce has been successful is reducing the fees charged by the ADRs, two out of seven major ADR providers continue to charge fees from individuals who file a complaint[47]. This represents the ADR providers used by about 20% of Safe Harbour companies. These companies have selected an ADR provider that charges a fee to consumers for filing a complaint. Such practices do not comply with the Enforcement Principle of Safe Harbour which gives individuals the right of access to a "readily available and affordable independent recourse mechanisms". In the European Union, access to an independent dispute resolution service provided by the EU Data Protection Panel is free for all data subjects.

On 12 November 2013 the Department of Commerce confirmed that it "will continue to advocate on behalf of EU citizens' privacy and work with ADR providers to determine whether their fees can be lowered further".

In relation to sanctions, not all ADR providers possess the necessary tools to remedy situations of failure to abide by the Privacy Principles. Moreover, the publication of findings

[46] For example, one major service provider ("TRUSTe") reported that it received 881 requests in 2010, but that only three of them were considered admissible, and grounded, and led to the company concerned being required to change its privacy policy and website. In 2011, the number of complaints was 879, and in one case the company was required to change its privacy policy. According to the DoC, vast majority of the complaints to ADR are requests from consumers, for example users who have forgotten their password and were unable to obtain it from the internet service. Following Commission requests, the Department of Commerce developed new statistics reporting criteria to be used by all ADR. They distinguish between mere requests and complaints and they provide with further clarification of types of complaints received. These new criteria need however to be further discussed to make sure that new statistics in 2014 concern all ADR providers, are comparable and provide critical information to assess the effectiveness of the recourse mechanism.

[47] International Centre for Dispute Resolution / American Arbitration Association (ICDR/AAA), charges $ 200 and JAMS $ 250 "filing fee". The Department of Commerce informed the Commission that it had worked with the AAA, the most costly dispute resolution provider for individuals, to develop a Safe Harbour-specific program which reduced the cost to consumers from several thousands of dollars to a flat rate of $ 200.

of non-compliance does not seem to be foreseen amongst the range of sanctions and measures of all ADR service providers.

ADR providers are also required to refer cases to the Federal Trade Commission where a company fails to comply with the outcome of the ADR process, or rejects the ADR provider's decision, so that the Federal Trade Commission can review and investigate and, if appropriate, take enforcement measures. However, to date, there have been no cases of referral from ADR providers to the Federal Trade Commission for non-compliance[48].

Alternative dispute resolution service providers maintain on their Websites lists of companies (Dispute Resolution Participants) which use their services. This allows consumers to easily verify if – in case of dispute with a company – an individual can submit a complaint to an identified dispute resolution provider. Thus, for example the BBB dispute resolution provider lists all companies which are under the BBB dispute resolution system. However, there are numerous companies claiming to be under a specific dispute resolution system but not listed by the ADR service providers as participants of their dispute resolution scheme[49].

ADR mechanisms should be easily accessible, independent and affordable for individuals. A data subject should be able to file a complaint without any excessive constraints. All ADR bodies should publish on their websites statistics about the complaints handled as well as specific information about their outcome. Finally, the ADR bodies should be further monitored to make sure that information they provide about the procedure and how to lodge a complaint is clear and understandable, so that the dispute resolution becomes an effective, trusted mechanism providing results. It should also be reiterated that publication of findings of non-compliance should be included within the range of mandatory sanctions of ADRs.

6.2. Onward transfer

With the exponential growth of data flows there is a need to ensure the continued protection of personal data at all stages of data processing, notably when data is transferred by a company adhering to the Safe Harbour to a **third party processor**. Therefore, the need for the better enforcement of the Safe Harbour concerns not only Safe Harbour members but also subcontractors.

The Safe Harbour scheme allows onward transfers to third parties acting as "agents" if the company – member of the Safe Harbour scheme – "ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the Privacy Principles"[50]. For example, a cloud service provider is required by the Department of Commerce to enter into a contract even if it is "Safe Harbour-compliant" and it receives personal data for processing[51]. However, this provision is not clear in Annex II to the Safe Harbour Decision.

As the recourse to subcontractors has increased considerably over the past years, in particular in the context of cloud-computing, when entering such a contract, a Safe Harbour company

---

48 See FAQ 11.

49 Examples: Amazon has informed the DoC that it uses the BBB as its dispute resolution provider. However the BBB does not list Amazon among its dispute resolution participants. Vice versa, Arsalon Technologies (www.arsalon.net), a cloud hosting service provider, appears on the BBB Safe Harbour dispute resolution list but the company is not a current member of the Safe Harbour (situation as of 1 October 2013). BBB, TRUSTe and other ADR service providers should remove or correct the certification claims. They should be bound by an enforceable requirement to only certify companies who are members of the Safe Harbour.

50 See Commission Decision 2000/520/EC page 7 (onward transfer).

51 See: "Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing": http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf

should notify the Department of Commerce and be obliged to make public the privacy safeguards[52].

The three above mentioned issues: the alternative dispute resolution mechanism, reinforced oversight and onward transfers of data should be further clarified.

7. ACCESS TO DATA TRANSFERRED IN THE FRAMEWORK OF THE SAFE HARBOUR SCHEME

In the course of 2013, information on the scale and scope of US surveillance programmes has raised concerns over the continuity of protection of personal data lawfully transferred to the US under the Safe Harbour scheme. For instance, all companies involved in the PRISM programme, and which grant access to US authorities to data stored and processed in the US, appear to be Safe Harbour certified. This has made the Safe Harbour scheme one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the EU.

The Safe Harbour Decision provides, in Annex 1, that adherence to the Privacy Principles may be limited, if justified by national security, public interest, or law enforcement requirements or by statute, government regulation or case-law. In order for limitations and restrictions on the enjoyment of fundamental rights to be valid, they must be narrowly construed; they must be set forth in a publicly accessible law and they must be necessary and proportionate in a democratic society. In particular, the Safe Harbour Decision specifies that such limitations are allowed only **"to the extent necessary"** to meet national security, public interest, or law enforcement requirements[53]. While the exceptional processing of data for the purposes of national security, public interest or law enforcement is provided under the Safe Harbour scheme, the large scale access by intelligence agencies to data transferred to the US in the context of commercial transactions was not foreseeable at the time of adopting the Safe Harbour.

Moreover, for reasons of transparency and legal certainty, the European Commission should be notified by the Department of Commerce of any statute or government regulations that would affect adherence to the Safe Harbour Privacy Principles[54]. The use of exceptions should be carefully monitored and the exceptions must not be used in a way that undermines the protection afforded by the **Principles**[55]. In particular, large scale access by US authorities to data processed by Safe Harbour self-certified companies risks undermining the confidentiality of electronic communications.

---

52 These remarks concern cloud providers which are not in the Safe Harbour. According to Galexia consultancy firm, "the level of Safe Harbour membership (and compliance) amongst cloud service providers is quite high. Cloud service providers typically have multiple layers of privacy protection, often combining direct contracts with clients and over-arching privacy policies. With one or two important exceptions, cloud service providers in the Safe Harbour are compliant with the key provisions relating to dispute resolution and enforcement. There are no major cloud service providers in the list of false membership claims at this time." (appearance of Chris Connolly from Galexia before the LIBE Committee inquiry on "Electronic mass surveillance of EU citizens").

53 See Annex 1 of the Safe Harbour Decision: "Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive of Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible."

54 Opinion 4/2000 on the level of protection provided by the "Safe Harbour Principles", adopted by Article 29 Data Protection Working Party on 16 May 2000.

55 Opinion 4/2000 on the level of protection provided by the "Safe Harbour Principles", adopted by Article 29 Data Protection Working Party on 16 May 2000.

7.1. Proportionality and necessity

As results from the findings of the ad hoc EU-US Working Group on data protection, a number of legal bases under US law allow large-scale collection and processing of personal data that is stored or otherwise processed companies based in the US. This may include data previously transferred from the EU to the US under the Safe Harbour scheme, and it raises the question of continued compliance with the Safe Harbour principles. The large scale nature of these programmes may result in data transferred under Safe Harbour being accessed and further processed by US authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in the Safe Harbour Decision.

7.2. Limitations and redress possibilities

As results from the findings of the ad hoc EU-US Working Group on data protection, safeguards that are provided under US law are mostly available to US citizens or legal residents. Moreover, there are no opportunities for either EU or US data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the US surveillance programmes.

7.3. Transparency

Companies do not systematically indicate in their privacy policies when they apply exceptions to the Principles. The individuals and companies are thus not aware of what is being done with their data. This is particularly relevant in relation with the operation of the US surveillance programmes in question. As a result, Europeans whose data are transferred to a company in the US under Safe Harbour may not be made aware by those companies that their data may be subject to access[56]. This raises the question of compliance with the Safe Harbour principles on transparency. Transparency should be ensured to the greatest extent possible without jeopardising national security. In addition to existing requirements on companies to indicate in their privacy policies where the Principles may be limited by statute, government regulation or case law, companies should also be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.

8. CONCLUSIONS AND RECOMMENDATIONS

Since its adoption in 2000, Safe Harbour has become a vehicle for EU-US flows of personal data. The importance of efficient protection in case of transfers of personal data has increased due to the exponential increase in data flows central to the digital economy and the very significant developments in data collection, processing and use. Web companies such as Google, Facebook, Microsoft, Apple, Yahoo have hundreds of millions of clients in Europe and transfer personal data for processing to the US on a scale inconceivable in the year 2000 when the Safe Harbour was created.

---

[56] Relatively transparent information in this respect is provided by some European companies in Safe Harbour. For example Nokia, which has operations in the US and is a Safe Harbour member provides a following notice in its privacy policy: *"We may be obligated by mandatory law to disclose your personal data to certain authorities or other third parties, for example, to law enforcement agencies in the countries where we or third parties acting on our behalf operate."*

Due to deficiencies in transparency and enforcement of the arrangement, specific problems still persist and should be addressed:

a) transparency of privacy policies of Safe Harbour members,

b) effective application of Privacy Principles by companies in the US, and

c) effectiveness of the enforcement.

Furthermore, the **large scale access by intelligence agencies to data transferred to the US by Safe Harbour certified companies** raises additional serious questions regarding the continuity of data protection rights of Europeans when their data in transferred to the US.

On the basis of the above, the Commission has identified the following **recommendations**:

Transparency

1. *Self-certified companies should publicly disclose their privacy policies.* It is not sufficient for companies to provide the Department of Commerce with a description of their privacy policy. Privacy policies should be made publicly available on the companies' websites, in clear and conspicuous language.
2. *Privacy policies of self-certified companies' websites should always include a link to the Department of Commerce Safe Harbour website which lists all the 'current' members of the scheme.* This will allow European data subjects to verify immediately, without additional searches whether a company is currently a member of the Safe Harbour. This would help increase the credibility of the scheme by reducing the possibilities for false claims of adherence to the Safe Harbour. The Department of Commerce has started in March 2013 to request this from companies, but the process should be intensified.
3. *Self-certified companies should publish privacy conditions of any contracts they conclude with subcontractors, e.g. cloud computing services.* Safe Harbour allows onward transfers from Safe Harbour self-certified companies to third parties acting as "agents", for example to cloud service providers. According to our understanding, in such cases the Department of Commerce requires from self-certified companies to enter into a contract. However, when entering such a contract, a Safe Harbour company should also notify the Department of Commerce and be obliged to make public the privacy safeguards.
4. *Clearly flag on the website of the Department of Commerce all companies which are not current members of the scheme.* The label "Not current" on the Department of Commerce list of Safe Harbour members should be accompanied by a clear warning that a company is currently not fulfilling Safe Harbour requirements. However, in the case of "Not current" the company is obliged to continue to apply the Safe Harbour requirements for the data that has been received under Safe Harbour.

Redress

5. *The privacy policies on companies' websites should include a link to the alternative dispute resolution (ADR) provider and/or EU panel.* This will allow European data subjects to contact immediately the ADR or EU panel in case of problems. Department of Commerce has started in March 2013 to request this from companies, but the process should be intensified.

6. *ADR should be readily available and affordable.* Some ADR bodies in the Safe Harbour scheme continue to charge fees from individuals – which can be quite costly for an individual user – for the handling of the complaint ($ 200-250). By contrast, in Europe access to the Data Protection Panel foreseen for solving complaints under the Safe Harbour, is free.

7. *Department of Commerce should monitor more systematically ADR providers regarding the transparency and accessibility of information they provide concerning the procedure they use and the follow-up they give to complaints.* This makes the dispute resolution an effective, trusted mechanism providing results. It should also be reiterated that publication of findings of non-compliance should be included within the range of mandatory sanctions of ADRs.

Enforcement

8. *Following the certification or recertification of companies under the Safe Harbour, a certain percentage of these companies should be subject to ex officio investigations of effective compliance of their privacy policies (going beyond control of compliance with formal requirements).*

9. *Whenever there has been a finding of non-compliance, following a complaint or an investigation, the company should be subject to follow-up specific investigation after 1 year.*

10. *In case of doubts about a company's compliance or pending complaints, the Department of Commerce should inform the competent EU data protection authority.*

11. *False claims of Safe Harbour adherence should continue to be investigated.* A company claiming on its website that it complies with the Safe Harbour requirements, but is not listed by the Department of Commerce as a 'current' member of the scheme, is misleading consumers and abusing their trust. False claims weaken the credibility of the system as a whole and therefore should be immediately removed from the companies' websites.

Access by US authorities

12. *Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.*

13. *It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate.*

Date de réception : 23/01/2015

Published ID	:	C-362/14
Document number	:	13
Register number	:	976996
Date of lodgment	:	03/11/2014
Date of entry in the register	:	03/11/2014
Type of document	:	Observations
	:	Annexes Part 3
Lodgment reference	:	DC33346
File number	:	4
Person lodging document	:	Julie Vondung (R249125) Commission

Annex 3

Communication from the Commission to the European Parliament and the Council, "Rebuilding Trust in EU-US Data Flows", COM(2013) 846, 27.11.2013, referred to in paragraphs 29 and 30 of the observations.

EUROPEAN
COMMISSION

Brussels, 27.11.2013
COM(2013) 846 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Rebuilding Trust in EU-US Data Flows

1. INTRODUCTION: THE CHANGING ENVIRONMENT OF EU-US DATA PROCESSING

The European Union and the United States are strategic partners, and this partnership is critical for the promotion of our shared values, our security and our common leadership in global affairs.

However, trust in the partnership has been negatively affected and needs to be restored. The EU, its Member States and European citizens have expressed deep concerns at revelations of large-scale US intelligence collection programmes, in particular as regards the protection of personal data[1]. Mass surveillance of private communication, be it of citizens, enterprises or political leaders, is unacceptable.

Transfers of personal data are an important and necessary element of the transatlantic relationship. They form an integral part of commercial exchanges across the Atlantic including for new growing digital businesses, such as social media or cloud computing, with large amounts of data going from the EU to the US. They also constitute a crucial component of EU-US co-operation in the law enforcement field, and of the cooperation between Member States and the US in the field of national security. In order to facilitate data flows, while ensuring a high level of data protection as required under EU law, the US and the EU have put in place a series of agreements and arrangements.

Commercial exchanges are addressed by Decision 2000/520/EC[2] (hereafter "the Safe Harbour Decision"). This Decision provides a legal basis for transfers of personal data from the EU to companies established in the US which have adhered to the Safe Harbour Privacy Principles.

Exchange of personal data between the EU and the US for the purposes of law enforcement, including the prevention and combating of terrorism and other forms of serious crime, is governed by a number of agreements at EU level. These are the Mutual Legal Assistance Agreement[3], the Agreement on the use and transfer of Passenger Name Records (PNR)[4], the Agreement on the processing and transfer of Financial Messaging Data for the purpose of the Terrorist Finance Tracking Program (TFTP)[5], and the Agreement between Europol and the US. These Agreements respond to important security challenges and meet the common security interests of the EU and US, whilst providing a high level of protection of personal data. In addition, the EU and the US are currently negotiating a framework agreement on data protection in the field of police and judicial cooperation ("umbrella agreement")[6]. The aim is to ensure a high level of data protection for citizens whose data is exchanged thereby further

---

1 For the purposes of this Communication, references to EU citizens include also non-EU data subjects which fall within the scope of European Union's data protection law.

2 Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, p. 7.

3 Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 291, 7.11. 2009, p. 40.

4 Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L215, 11.8.2012, p. 4.

5 Council Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ L 195, 27.7.2010, p. 3.

6 The Council adopted the Decision authorising the Commission to negotiating the Agreement on 3 December 2010. See IP/10/1661 of 3 December 2010.

advancing EU-US cooperation in the combating of crime and terrorism on the basis of shared values and agreed safeguards.
These instruments operate in an environment in which personal data flows are acquiring increasing relevance.
On the one hand, the development of the digital economy has led to exponential growth in the quantity, quality, diversity and nature of data processing activities. The use of electronic communication services by citizens in their daily lives has increased. Personal data has become a highly valuable asset: the estimated value of EU citizens' data was €315bn in 2011 and has the potential to grow to nearly €1tn annually by 2020[7]. The market for the analysis of large sets of data is growing by 40% per year worldwide[8]. Similarly, technological developments, for example related to cloud computing, put into perspective the notion of international data transfer as cross-border data flows are becoming a day to day reality.[9]
The increase in the use of electronic communications and data processing services, including cloud computing, has also substantially expanded the scope and significance of transatlantic data transfers. Elements such as the central position of US companies in the digital economy[10], the transatlantic routing of a large part of electronic communications and the volume of electronic data flows between the EU and the US have become even more relevant.
On the other hand, modern methods of personal data processing raise new and important questions. This applies both to new means of large-scale processing of consumer data by private companies for commercial purposes, and to the increased ability of large-scale surveillance of communications data by intelligence agencies.
Large-scale US intelligence collection programmes, such as PRISM affect the fundamental rights of Europeans and, specifically, their right to privacy and to the protection of personal data. These programmes also point to a connection between Government surveillance and the processing of data by private companies, notably by US internet companies. As a result, they may therefore have an economic impact. If citizens are concerned about the large-scale processing of their personal data by private companies or by the surveillance of their data by intelligence agencies when using Internet services, this may affect their trust in the digital economy, with potential negative consequences on growth.
These developments expose EU-US data flows to new challenges. This Communication addresses these challenges. It explores the way forward on the basis of the findings contained in the Report of the EU Co-Chairs of the ad hoc EU-US Working Group and the Communication on the Safe Harbour.
It seeks to provide an effective way forward to rebuild trust and reinforce EU-US cooperation in these fields and strengthen the broader transatlantic relationship.

This Communication is based on the premise that the standard of protection of personal data must be addressed in its proper context, without affecting other dimensions of EU-US relations, including the on-going negotiations for a Transatlantic Trade and Investment Partnership. For this reason, data protection standards will not be negotiated within the Transatlantic Trade and Investment Partnership, which will fully respect the data protection rules.

---

7 See Boston Consulting Group, "The Value of our Digital Identity", November 2012.
8 See McKinsey, "Big data: The next frontier for innovation, competition, and productivity", 2011
9 Communication on Unleashing the potential of cloud computing in Europe,COM(2012) 529 final
10 For example, the combined number of unique visitors to Microsoft Hotmail, Google Gmail and Yahoo! Mail from European countries in June 2012 totalled over 227 million, eclipsing that of all other providers. The combined number of unique European users accessing Facebook and Facebook Mobile in March 2012 was 196.5 million, making Facebook the largest social network in Europe. Google is the leading internet search engine with 90.2% of worldwide internet users. US mobile messaging service What's App was used by 91% of iPhone users in Germany in June 2013.

It is important to note that whilst the EU can take action in areas of EU competence, in particular to safeguard the application of EU law[11], national security remains the sole responsibility of each Member State[12].

2. THE IMPACT ON THE INSTRUMENTS FOR DATA TRANSFERS

First, as regards data transferred for commercial purposes, the Safe Harbour has proven to be an important vehicle for EU-US data transfers. Its commercial importance has grown as personal data flows have taken on greater prominence in the transatlantic commercial relationship. Over the past 13 years, the Safe Harbour scheme has evolved to include more than 3.000 companies, over half of which have signed up within the last five years. Yet concerns about the level of protection of personal data of EU citizens transferred to the US under the Safe Harbour scheme have grown. The voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement. While a majority of US companies apply its principles, some self-certified companies do not. The non-compliance of some self-certified companies with the Safe Harbour Privacy Principles places such companies at a competitive advantage in relation to European companies operating in the same markets.

Moreover, while under the Safe Harbour, limitations to data protection rules are permitted where necessary on grounds of national security[13], the question has arisen whether the large-scale collection and processing of personal information under US surveillance programmes is necessary and proportionate to meet the interests of national security. It is also clear from the findings of the ad hoc EU-US Working Group that, under these programmes, EU citizens do not enjoy the same rights and procedural safeguards as Americans.

The reach of these surveillance programmes, combined with the unequal treatment of EU citizens, brings into question the level of protection afforded by the Safe Harbour arrangement. The personal data of EU citizens sent to the US under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the EU and the purposes for which it was transferred to the US. A majority of the US internet companies that appear to be more directly concerned by these programmes are certified under the Safe Harbour scheme.

Second, as regards exchanges of data for law enforcement purposes, the existing Agreements (PNR, TFTP) have proven highly valuable tools to address common security threats linked to serious transnational crime and terrorism, whilst laying down safeguards that ensure a high level of data protection[14]. These safeguards extend to EU citizens, and the Agreements provide for mechanisms to review their implementation and to address issues of concern related thereto. The TFTP Agreement also establishes a system of oversight, with EU independent overseers checking how data covered by the Agreement is searched by the US.

Against the backdrop of concerns raised in the EU about US surveillance programmes, the European Commission has used those mechanisms to check how the agreements are applied. In the case of the PNR Agreement, a joint review was conducted, involving data protection

---

11 See Judgment of the Court of Justice of the European Union in Case C-300/11, ZZ v Secretary of State for the Home Department.

12 Article 4(2) TEU.

13 See e.g. Safe Harbour Decision, Annex I.

14 See Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.

experts from the EU and the US, looking at how the Agreement has been implemented[15]. That review did not give any indication that US surveillance programmes extend to or have impact on the passenger data covered by the PNR Agreement. In the case of the TFTP Agreement, the Commission opened formal consultations after allegations were made of US intelligence agencies directly accessing personal data in the EU, contrary to the Agreement. These consultations did not reveal any elements proving a breach of the TFTP Agreement, and they led the US to provide written assurance that no direct data collection has taken place contrary to the provisions of the Agreement.

The large-scale collection and processing of personal information under US surveillance programmes call, however, for a continuation of very close monitoring of the implementation of the PNR and TFTP Agreements in the future. The EU and the US have therefore agreed to advance the next Joint Review of the TFTP Agreement, which will be held in Spring 2014. Within that and future joint reviews, greater transparency will be ensured on how the system of oversight operates and on how it protects the data of EU citizens. In parallel, steps will be taken to ensure that the system of oversight continues to pay close attention to how data transferred to the US under the Agreement is processed, with a focus on how such data is shared between US authorities.

Third, the increase in the volume of processing of personal data underlines the importance of the legal and administrative safeguards that apply. One of the goals of the Ad Hoc EU-US Working Group was to establish what safeguards apply to minimise the impact of the processing on the fundamental rights of EU citizens. Safeguards are also necessary to protect companies. Certain US laws such as the Patriot Act, enable US authorities to directly request companies access to data stored in the EU. Therefore, European companies, and US companies present in the EU, may be required to transfer data to the US in breach of EU and Member States' laws, and are consequently caught between conflicting legal obligations. Legal uncertainty deriving from such direct requests may hold back the development of new digital services, such as cloud computing, which can provide efficient, lower-cost solutions for individuals and businesses.

3. ENSURING THE EFFECTIVENESS OF DATA PROTECTION

Transfers of personal data between the EU and the US are an essential component of the transatlantic commercial relationship. Information sharing is also an essential component of EU-US security cooperation, critically important to the common goal of preventing and combating serious crime and terrorism. However, recent revelations about US intelligence collection programmes have negatively affected the trust on which this cooperation is based. In particular, it has affected trust in the way personal data is processed. The following steps should be taken to restore trust in data transfers for the benefit of the digital economy, security both in the EU and in the US, and the broader transatlantic relationship.

3.1. The EU data protection reform

The data protection reform proposed by the Commission in January 2012[16] provides a key response as regards the protection of personal data. Five components of the proposed Data Protection package are of particular importance.

---

[15] See on the Commission report "Joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security".

[16] COM(2012) 10 final: Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.1.2012, and COM(2012) 11 final: Proposal for a Regulation of the European Parliament and the Council on the protection of individuals

First, as regards territorial scope, the proposed regulation makes clear that companies that are not established in the Union will have to apply EU data protection law when they offer goods and services to European consumers or monitor their behaviour. In other words, the fundamental right to data protection will be respected, independently of the geographical location of a company or of its processing facility[17].
Secondly, on international transfers, the proposed regulation establishes the conditions under which data can be transferred outside the EU. Transfers can only be allowed where these conditions, which safeguard the individuals' rights to a high level of protection, are met[18].
Thirdly, concerning enforcement, the proposed rules provide for proportionate and dissuasive sanctions (up to 2% of a company's annual global turnover) to make sure that companies comply with EU law[19]. The existence of credible sanctions will increase companies' incentive to comply with EU law.
Fourthly, the proposed regulation includes clear rules on the obligations and liabilities of data processors such as cloud providers, including on security[20]. As the revelations about US intelligence collection programmes have shown, this is critical because these programmes affect data stored in the cloud. Also, companies providing storage space in the cloud which are asked to provide personal data to foreign authorities will not be able to escape their responsibility by reference to their status as data processors rather than data controllers.
Fifth, the package will lead to the establishment of comprehensive rules for the protection of personal data processed in the law enforcement sector.
It is expected that the package will be agreed upon in a timely manner in the course of 2014[21].

3.2. Making Safe Harbour safer

The Safe Harbour scheme is an important component of the EU-US commercial relationship, relied upon by companies on both sides of the Atlantic.
The Commission's report on the functioning of Safe Harbour has identified a number of weaknesses in the scheme. As a result of a lack of transparency and of enforcement, some self-certified Safe Harbour members do not, in practice, comply with its principles. This has a negative impact on EU citizens' fundamental rights. It also creates a disadvantage for European companies compared to those competing US companies that are operating under the scheme but in practice not applying its principles. This weakness also affects the majority of US companies which properly apply the scheme. Safe Harbour also acts as a conduit for the

---

with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

17 The Commission takes note that the European Parliament confirmed and strengthened this important principle, enshrined in Art. 3 of the proposed Regulation, in its vote of 21 October 2013 on the data protection reform reports of MEPs Jan-Philipp Albrecht and Dimitrios Droutsas in the Committee for Civil Liberties, Justice and Home Affairs (LIBE).

18 The Commission takes note that in its vote of 21 October 2013, the LIBE Committee of the European Parliament proposed to include a provision in the future Regulation that would subject requests from foreign authorities to access personal data collected in the EU to the obtaining of a prior authorisation from a national data protection authority, where such a request would be issued outside a mutual legal assistance treaty or another international agreement.

19 The Commission takes note that in its vote of 21 October 2013, the LIBE Committee proposed strengthening the Commission's proposal by providing that fines can go up to 5% of the annual worldwide turnover of a company.

20 The Commission takes note that in its vote of 21 October 2013, the LIBE Committee endorsed the strengthening of the obligations and liabilities of data processors, in the particular with regard to Art. 26 of the proposed Regulation.

21 The Conclusions of the October 2013 European Council state that: "It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015".

transfer of the personal data of EU citizens from the EU to the US by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes. Unless the deficiencies are corrected, it therefore constitutes a competitive disadvantage for EU business and has a negative impact on the fundamental right to data protection of EU citizens.

The shortcomings of the Safe Harbour scheme have been underlined by the response of European Data Protection Authorities to the recent surveillance revelations. Article 3 of the Safe Harbour Decision authorises these authorities to suspend, under certain conditions, data flows to certified companies.[22] German data protection commissioners have decided not to issue new permissions for data transfers to non-EU countries (for example for the use of certain cloud services). They will also examine whether data transfers on the basis of the Safe Harbour should be suspended.[23] The risk is that such measures, taken at national level, would create differences in coverage, which means that Safe Harbour would cease to be a core mechanism for the transfer of personal data between the EU and the US.

The Commission has the authority under Directive 95/46/EC to suspend or revoke the Safe Harbour decision if the scheme no longer provides an adequate level of protection. Furthermore, Article 3 of the Safe Harbour Decision provides that the Commission may reverse, suspend or limit the scope of the decision, while, under article 4, it may adapt the decision at any time in the light of experience with its implementation.

Against this background, a number of policy options can be considered, including:

- Maintaining the *status quo*;
- Strengthening the Safe Harbour scheme and reviewing its functioning thoroughly;
- Suspending or revoking the Safe Harbour decision.

Given the weaknesses identified, the current implementation of Safe Harbour cannot be maintained. However, its revocation would adversely affect the interests of member companies in the EU and in the US. The Commission considers that Safe Harbour should rather be strengthened.

The improvements should address both the structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception.

More specifically, for Safe Harbour to work as intended, the monitoring and supervision by US authorities of the compliance of certified companies with the Safe Harbour Privacy Principles needs to be more effective and systematic. The transparency of certified companies' privacy policies needs to be improved. The availability and affordability of dispute resolution mechanisms also needs to be ensured to EU citizens.

As a matter of urgency, the Commission will engage with the US authorities to discuss the shortcomings identified. Remedies should be identified by summer 2014 and implemented as soon as possible. On the basis thereof, the Commission will undertake a complete stock taking of the functioning of the Safe Harbour. This broader review process should involve open consultation and a debate in the European Parliament and the Council as well as discussions with the US authorities.

---

22 Specifically, pursuant to Art. 3 of the Safe Harbour Decision, such suspensions may take place in cases where there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

23 Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, press release of 24 July 2013.

It is also important that the national security exception foreseen by the Safe Harbour Decision, is used only to an extent that is strictly necessary and proportionate.

3.3. Strengthening data protection safeguards in law enforcement cooperation

The EU and the US are currently negotiating a data protection "umbrella" agreement on transfers and processing of personal information in the context of police and judicial co-operation in criminal matters. The conclusion of such an agreement providing for a high level of protection of personal data would represent a major contribution to strengthening trust across the Atlantic. By advancing the protection of EU data citizens' rights, it would help strengthen transatlantic cooperation aimed at preventing and combating crime and terrorism.

According to the decision authorising the Commission to negotiate the umbrella agreement, the aim of the negotiations should be to ensure a high level of protection in line with the EU data protection *acquis*. This should be reflected in agreed rules and safeguards on, *inter alia*, purpose limitation, the conditions and the duration of the retention of data. In the context of the negotiation, the Commission should also obtain commitments on enforceable rights including judicial redress mechanisms for EU citizens not resident in the US[24]. Close EU-US cooperation to address common security challenges should be mirrored by efforts to ensure that citizens benefit from the same rights when the same data is processed for the same purposes on both sides of the Atlantic. It is also important that derogations based on national security needs are narrowly defined. Safeguards and limitations should be agreed in this respect.

These negotiations provide an opportunity to clarify that personal data held by private companies and located in the EU will not be directly accessed by or transferred to US law enforcement authorities outside of formal channels of co-operation, such as Mutual Legal Assistance agreements or sectoral EU-US Agreements authorising such transfers. Access by other means should be excluded, unless it takes place in clearly defined, exceptional and judicially reviewable situations. The US should undertake commitments in that regard[25].

An "umbrella agreement" agreed along those lines, should provide the general framework to ensure a high level of protection of personal data when transferred to the US for the purpose of preventing or combating crime and terrorism. Sectoral agreements should, where necessary due to the nature of the data transfer concerned, lay down additional rules and safeguards, building on the example of the EU-US PNR and TFTP Agreements, which set strict conditions for transfer of data and safeguards for EU citizens.

---

[24] See the relevant passage of the Joint Press Statement following the EU-US-Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: "We are therefore, as a matter of urgency, committed to advancing rapidly in the negotiations on a meaningful and comprehensive data protection umbrella agreement in the field of law enforcement. The agreement would act as a basis to facilitate transfers of data in the context of police and judicial cooperation in criminal matters by ensuring a high level of personal data protection for U.S. and EU citizens. We are committed to working to resolve the remaining issues raised by both sides, including judicial redress (a critical issue for the EU). Our aim is to complete the negotiations on the agreement ahead of summer 2014."

[25] See the relevant passage of the Joint Press Statement following the EU-US Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: "We also underline the value of the EU-U.S. Mutual Legal Assistance Agreement. We reiterate our commitment to ensure that it is used broadly and effectively for evidence purposes in criminal proceedings. There were also discussions on the need to clarify that personal data held by private entities in the territory of the other party will not be accessed by law enforcement agencies outside of legally authorized channels. We also agree to review the functioning of the Mutual Legal Assistance Agreement, as contemplated in the Agreement, and to consult each other whenever needed."

3.4. Addressing European concerns in the on-going US reform process

US President Obama has announced a review of US national security authorities' activities, including of the applicable legal framework. This on-going process provides an important opportunity to address EU concerns raised by recent revelations about US intelligence collection programmes. The most important changes would be extending the safeguards available to US citizens and residents to EU citizens not resident in the US, increased transparency of intelligence activities, and further strengthening oversight. Such changes would restore trust in EU-US data exchanges, and promote the use of Internet services by Europeans.

With respect to extending the safeguards available to US citizens and residents to EU citizens, legal standards in relation to US surveillance programmes which treat US and EU citizens differently should be reviewed, including from the perspective of necessity and proportionality, keeping in mind the close transatlantic security partnership based on common values, rights and freedoms. This would reduce the extent to which Europeans are affected by US intelligence collection programmes.

More transparency is needed on the legal framework of US intelligence collection programmes and its interpretation by US Courts as well as on the quantitative dimension of US intelligence collection programmes. EU citizens would also benefit from such changes.

The oversight of US intelligence collection programmes would be improved by strengthening the role of the Foreign Intelligence Surveillance Court and by introducing remedies for individuals. These mechanisms could reduce the processing of personal data of Europeans that are not relevant for national security purposes.

3.5. Promoting privacy standards internationally

Issues raised by modern methods of data protection are not limited to data transfer between the EU and the US. A high level of protection of personal data should also be guaranteed to any individual. EU rules on collection, processing and transfer of data should be promoted internationally.

Recently, a number of initiatives have been proposed to promote the protection of privacy, particularly on the internet[26]. The EU should ensure that such initiatives, if pursued, fully take into account the principles of protecting fundamental rights, freedom of expression, personal data and privacy as set out in EU law and in the EU Cyber Security Strategy, and do not undermine the freedom, openness and security of cyber space. This includes a democratic and efficient multi stakeholder governance model.

The on-going reforms of data protection laws on both sides of the Atlantic also provide the EU and the US a unique opportunity to set the standard internationally. Data exchanges across the Atlantic and beyond would greatly benefit from the strengthening of the US domestic legal framework, including the passage of the "Consumer Privacy Bill of Rights" announced by President Obama in February 2012 as part of a comprehensive blueprint to improve consumers' privacy protections. The existence of a set of strong and enforceable data protection rules enshrined in both the EU and the US would constitute a solid basis for cross-border data flows.

In view of promoting privacy standards internationally, accession to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), which is open to countries which are not member of the Council of Europe[27], should also be favoured. Safeguards and guarantees agreed in international fora should result in a high level of protection compatible with what is required under EU law.

---

[26] See in this respect the draft resolution proposed to the UN General Assembly by Germany and Brazil – calling for the protection of privacy online as offline.

[27] The US is already party to another Council of Europe convention: the 2001 Convention on Cybercrime (also known as the "Budapest Convention").

4. CONCLUSIONS AND RECOMMENDATIONS

The issues identified in this Communication require action to be taken by the US as well as by the EU and its Member States.

The concerns around transatlantic data exchanges are, first of all, a wake-up call for the EU and its Member States to advance swiftly and with ambition on the data protection reform. It shows that a strong legislative framework with clear rules that are enforceable also in situations when data are transferred abroad is, more than ever, a necessity. The EU institutions should therefore continue working towards the adoption of the EU data protection reform by spring 2014, to make sure that personal data is effectively and comprehensively protected.

Given the significance of transatlantic data flows, it is essential that the instruments on which these exchanges are based appropriately address the challenges and opportunities of the digital era and new technological developments like cloud computing. Existing and future arrangements and agreements should ensure that the continuity of a high level of protection is guaranteed over the Atlantic.

A robust Safe Harbour scheme is in the interests of EU and US citizens and companies. It should be strengthened by better monitoring and implementation in the short term, and, on this basis, by a broader review of its functioning. Improvements are necessary to ensure that the original objectives of the Safe Harbour Decision – i.e. continuity of data protection, legal certainty and free EU-US flow of data – are still met.

These improvements should focus on the need for the US authorities to better supervise and monitor the compliance of self-certified companies with the Safe Harbour Privacy Principles.

It is also important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary and proportionate.

In the area of law enforcement, the current negotiations of an "umbrella agreement" should result in a high level of protection for citizens on both sides of the Atlantic. Such an agreement would strengthen the trust of Europeans in EU-US data exchanges, and provide a basis to further develop EU-US security cooperation and partnership. In the context of the negotiation, commitments should be secured to the effect that procedural safeguards, including judicial redress, are available to Europeans who are not resident in the US.

Commitments should be sought from the US administration to ensure that personal data held by private entities in the EU will not be accessed directly by US law enforcement agencies outside of formal channels of co-operation, such as Mutual Legal Assistance agreements and sectoral EU-US Agreements such as PNR and TFTP authorising such transfers under strict conditions, except in clearly defined, exceptional and judicially reviewable situations.

The US should also extend the safeguards available to US citizens and residents to EU citizens not resident in the US, ensure the necessity and proportionality of the programmes, greater transparency and oversight in the legal framework applicable to US national security authorities.

Areas listed in this communication will require constructive engagement from both sides of the Atlantic. Together, as strategic partners, the EU and the US have the ability to overcome the current tensions in the transatlantic relationship and rebuild trust in EU-US data flows. Undertaking joint political and legal commitments on further cooperation in these areas will strengthen the overall transatlantic relationship.